

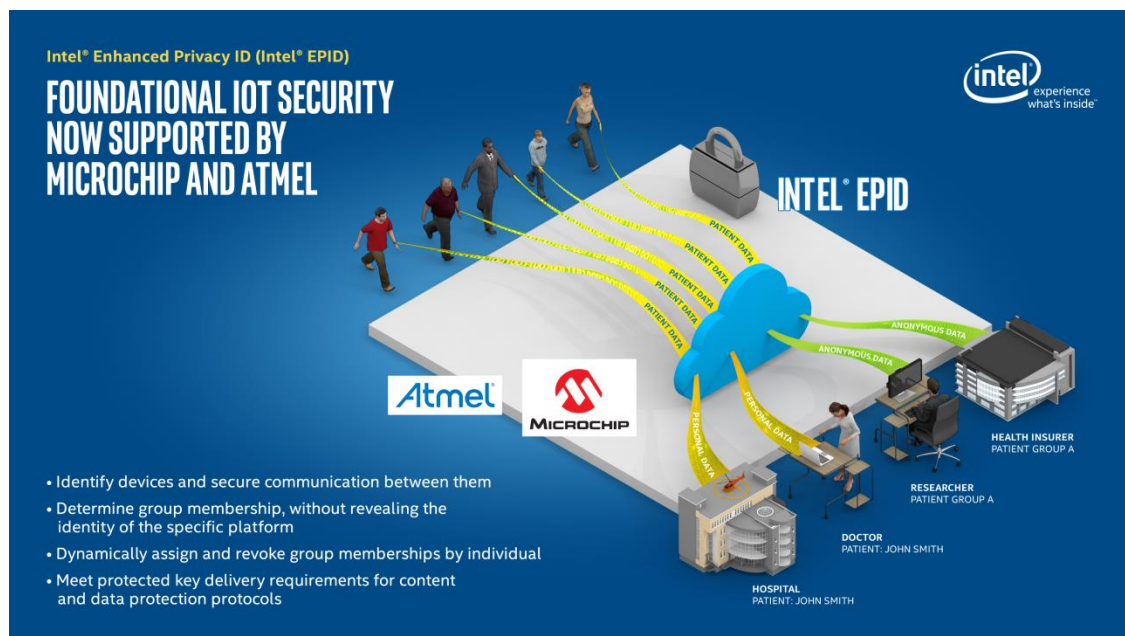
Atmel and Microchip Adopt Intel Identity Technology for IoT

Companies Collaborate to Provide Intel Enhanced Privacy ID (EPID) Technology as a Common Security Foundation for IoT Platforms

Aug. 18, 2015 — Intel today announced that its Enhanced Privacy ID (Intel® EPID) identity technology is being adopted by [Microchip*](#) and [Atmel*](#) to help improve interoperability in securing Internet of Things (IoT) solutions. The companies join an ecosystem where more than 1.1 billion Intel EPID certificates have been deployed.

IoT is expected to be a multitrillion-dollar market with an installed base of 50 billion connected things by the end of 2020, but the industry faces hurdles in implementing IoT solutions due to challenges with security, interoperability and solution complexity. By using Intel EPID as a security baseline across the network, the ecosystem can enable different solutions to more securely connect with one another and drive the Internet of Things to scale.

Intel's EPID technology provides an "on-ramp" designed to help devices securely connect to the Intel® IoT Platform. Intel's EPID hardware-enforced integrity provides fixed device identity in a manner that is compatible with existing ISO and TCG standards, and helps protect privacy with sophisticated anonymity technology. Extending use of Intel EPID across the industry will help make IoT solutions more secure regardless of vendor choice.



Hardware-based Identity for Authentication and Anonymity

- Intel EPID allows developers to establish a basis for trust, authentication, inclusion in relevant system relationships, and authorization for data access and actuation. The solution uses a fixed, hardware-based identity built into the processor much like a person's fingerprints. Additionally,

the technology delivers device-based identity designed to provide anonymity, allowing devices to be verified as part of a group rather than by its individual private key.

- The technology helps protect personally identifiable information in connected devices, an essential aspect of future IoT solutions. For example, Intel EPID could potentially be used in a smart automotive solution to allow a car using an Intel EPID-enabled chip to connect to smart infrastructure without disclosing any information other than verification that it's part of a group of cars approved to access certain alerts, such as light changes and approaching emergency vehicles.
- Intel EPID can also offer an extra layer of security in case of a data security incident by providing system managers an easy way to manage group and device permissions in IoT deployments. By incorporating Intel EPID within the broader semiconductor industry, Intel aims to make this level of security broadly accessible and available.
- Intel contributed Intel EPID to ISO/IEC (20008 and 20009) and to TCG standards.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at <http://www.intel.com>.

Intel and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others. © 2015 Intel Corporation