WHITE PAPER

IoT Security

A Cost-Effective Foundation for End-to-End IoT Security

Intel® Enhanced Privacy ID (Intel® EPID) provides a proven, standards-based identity solution to help unleash the full growth potential of the IoT.

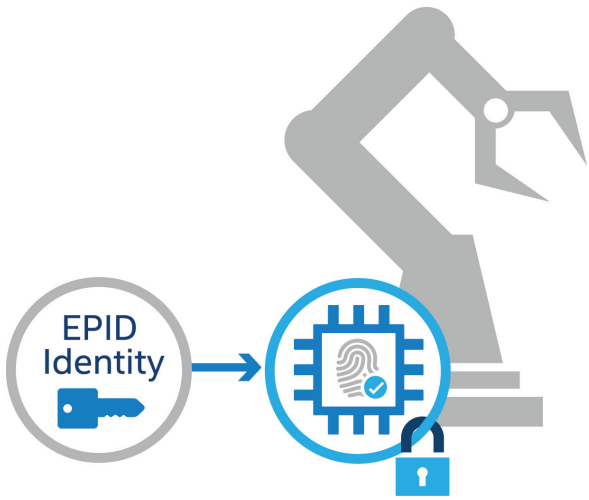

Table of Contents

Executive Summary

The Internet of Things (IoT) offers unprecedented opportunity for technology vendors, service providers, and the businesses and consumers they serve. Analysts are predicting a multi-trillion dollar IoT industry will emerge within the next five years, with tens of billions of connected devices expanding the power and reach of the Internet.

Of course, this enormous footprint of connected devices also offers an enormous new attack surface for hackers and malware. To create an environment of trust in which the IoT can truly thrive, security must be built into the IoT from the start. It must be strong, flexible, cost-effective, and massively scalable.

Intel® Enhanced Privacy ID (Intel® EPID) offers a proven foundation for addressing these needs. By providing immutable identity for every device, Intel EPID establishes a solid root of trust that can help to ensure that every device is a trusted device and every connection a trusted connection—all the way from end-point to cloud.

Intel EPID is easy to deploy and internationally standardized. It provides a flexible foundation for end-to-end IoT security that interoperates readily with existing software-based security solutions. It also provides unique privacy options that open the door to a wide range of new IoT usage models, enabling user anonymity and data protection to be flexibly tailored to the specific demands of each use case.

As the foundation for Intel's hardware-enhanced security technologies, more than 2.5 billion Intel EPID credentials have been issued since 2008. Every aspect of the technology has been proven at scale in the PC and server marketplace. Now Intel is making Intel EPID technology freely available to all silicon and device manufacturers, software vendors, and the broader IoT community. Intel is also working closely with leading IoT adopters, vendors, and cloud service providers (CSPs) to help them integrate Intel EPID into their products and services.

With its proven track record, broad datacenter footprint, and advanced privacy features, Intel EPID provides a clear path forward in an otherwise fragmented field of identity and security technologies. It can help IoT vendors and users develop solutions that not only generate and use data more effectively, but also protect it.

Security—A Fundamental Requirement for IoT Success

The Internet of Things (IoT) has been called the third wave of computing, and for good reason. As ubiquitous as the Internet has already become in our lives, the IoT will increase its penetration many fold. Connected sensors and smart devices in our homes, cars, workplaces, clothes, and accessories will generate massive amounts of new data, much of which will be filtered and analyzed in near real time to help us live safer, more productive, and more connected lives.

A Trusted Platform for IoT Innovation

Security is one barrier to IoT growth. Interoperability is another. To help break down both these obstacles, Intel has developed the Intel® IoT Platform, an end-to-end reference model for developing and deploying IoT solutions.

The Intel IoT Platform provides a comprehensive framework that works with Intel and third-party products to seamlessly and securely connect devices, deliver trusted data to the cloud, and provide high value through advanced data analytics. Using EPID as a foundation for identity, security, and privacy, the Intel IoT Platform helps vendors and users build their IoT solutions on a flexible, trusted foundation.

Learn more at: http://www.intel.com/content/www/us/en/internet-of-things/iot-platform.html

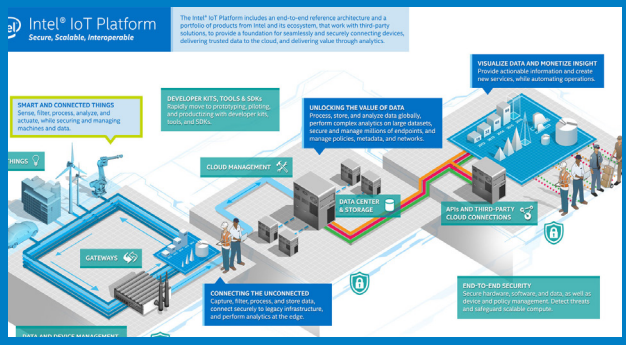

Figure 2 . Intel® IoT Platform Infographic

Intel has developed the Intel® IoT Platform reference model to simplify the development and deployment of advanced IoT solutions, and is now working directly with leading businesses such as Levi Strauss & Co., Honeywell, and Yanzi to design and implement high-value solutions across a range of industries (see sidebar, "A Trusted Platform for IoT Innovation"). The compelling value of these and many other IoT solutions is driving rapid growth in the IoT marketplace. Analysts predict the IoT will be a multitrillion dollar industry by 2020 and that there will be roughly 20-50 billion connected devices worldwide.

The ability to sustain this rapid growth depends, in large part, on the availability of interoperable and secure solutions that can be deployed cost-effectively. IoT solutions are becoming mission-critical for early adopters, yet security issues have already begun to emerge. White-hat hacks into self-driving cars, for example, have shined a light onto the risks that can arise when critical assets are monitored and controlled across public networks without adequate security safeguards.

To address the demands of such a complex and connected environment, security for IoT devices must be strong, distributed, and massively scalable. It must protect against unauthorized access to endpoints, gateways, networks, and cloud-based resources, and it must safeguard the integrity and privacy of both data and communications. Finally, security must be interoperable and affordable in order to support the fast, cost-effective build out of IoT solutions.

Intel EPID provides the foundation for addressing all these needs. This platform identity and authentication solution is widely supported, easy to deploy, standards-based, and proven at scale. It offers a trusted foundation on which to build end-to-end security solutions. It also provides unique privacy options that can help IoT users share data more flexibly across diverse scenarios, by tailoring the anonymity of users and the privacy of data to match the particular demands of each use case.

Laying the Foundation with Intel EPID

Intel has been focused on device security for decades, building hardware-enhanced security technologies into Intel processors and platforms to enable simpler, stronger security with less impact on performance, energy-consumption, and the user experience. Intel EPID provides the foundation for these security technologies. As a standards-based platform identity technology rooted in silicon, it establishes an isolated hardware root of trust that complements and strengthens other security safeguards such as software-based public key infrastructure (PKI) solutions.

Intel EPID offers a number of advantages over other identity solutions for IoT usage models. Since it is typically built into the silicon of a device, it can be supported at low cost and with relatively little effort. Provisioning is simple. Once devices are connected, they can be authenticated, registered, and provisioned over the network in a matter of minutes, using low-touch or even no-touch procedures. From the very first connection, technical personnel and management applications can be confident they are interacting with a trusted device, and, depending on the implementation, with a trusted software stack.

Immutable Identity for Every Device

Intel EPID authenticates platform identity through remote attestation using asymmetric (public and private key) cryptography. It can be implemented in hardware, software, or a combination of the two, so it can be used flexibly across a wide range of IoT use cases.

When implemented solely in software, Intel EPID provides levels of security that are comparable to other software-based cryptographic solutions, while also providing enhanced privacy options. When implemented partially or completely in hardware, Intel EPID provides an even stronger foundation for security. Private and public root keys are embedded in silicon during manufacturing and are stored and used only within a protected execution environment that is isolated from the main CPU, memory, and operating system of the device.

All core security operations are performed in the protected environment, which has its own processor, memory, and communication channels, and interacts with the rest of the platform only in limited, tightly-controlled ways. This isolation makes it extremely difficult, for security keys and certificates to be compromised by unauthorized applications or hackers. As a result, Intel EPID provides both immutable device identity and a trusted foundation for securing IoT hardware, software, and data.

Enhanced Privacy

In a standard PKI implementation, each public key has exactly one private key. Because of this one-to-one relationship, whenever a verifier uses a public key to authenticate a user, the user's identity is divulged. With Intel EPID, a single public key can have multiple private keys (typically millions). Verifiers authenticate the device as an anonymous member of the larger group, which protects the privacy of the user and device. See figure XX.

In practice, the privacy protections of Intel EPID go even deeper. Through the math of Elliptical Curve Cryptography, each private key is actually a large set of key values, and a single device can use a different key value in every transaction. This prevents anyone – including the manufacturer, the verifier, and the certificate authority – from tracing the key back to the root key or from identifying multiple transactions as emanating from the same device. Verifiers can only authenticate that the single transaction is being generated by a device that is a genuine member of the larger group.

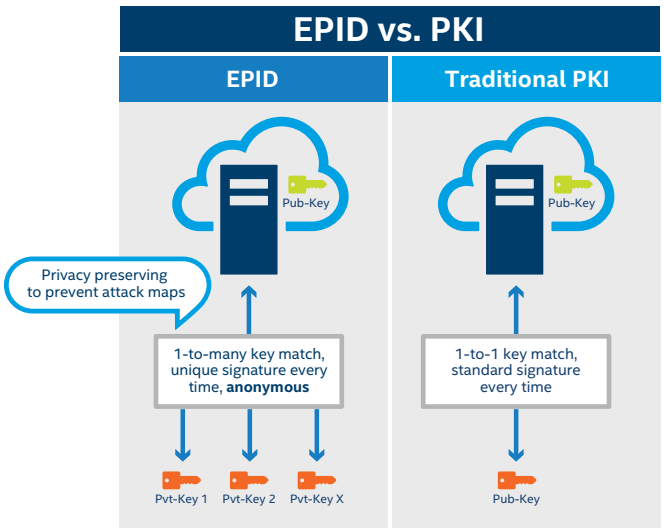

Figure 2. Comparison of Intel EPID to PKI

Although privacy is protected with Intel EPID, the use of privacy features is not required. If both parties agree, service providers can use Intel EPID to identify the transactions of a specific user or device. This would allow a provider, for example, to monitor and control a user's consumption of a premium service based on contractual agreements. However, this tracking option does not compromise privacy beyond the particular use case. Only the authorized service provider could identify multiple transactions as emanating from the same device.

This combination of enhanced privacy with optional, mutually-agreed-upon tracking provides the foundation for a wide range of anticipated IoT usage models (see the section, Unique Advantages for IoT Use Cases).

Flexible Revocation

In any large-scale IoT implementation, service providers or other verifiers must be able to revoke keys and certificates under a variety of circumstances, such as when a service contract is terminated, a device is repurposed, or a key or certificate becomes compromised. Intel EPID enables flexible revocation without sacrificing privacy. Three forms of revocation are supported. All are performed through the certificate authority (which could potentially be Intel or a third-party provider).

- Private key-based revocation. If a private key becomes exposed for any reason, the certificate authority can place that key on a revocation list to prevent further use.
- Signature-based revocation. If a signature is known, but the private key is not, the certificate authority can place the signature on a revocation list. This prevents future use of the key that was used to generate the signature, without exposing the key or the identity of the device.
- Group revocation. If a provider wishes to, they can revoke an entire group, either to terminate a service or to reconfigure the group key to improve security, performance, or manageability.

Unique Advantages for IoT Use Cases

As the IoT evolves, the immutable identity provided by Intel EPID, along with the ability to support anonymity, will become increasingly valuable. A few examples are described below.

No-Touch Device Registration and Provisioning

Enterprises and service providers may ultimately have hundreds to thousands of gateways and thousands to millions of sensors, actuators, and other devices. To support security at this scale, identity solutions must be simple and cost-effective to implement. However, most available IoT identity solutions require manual registration and provisioning in the field, a process that can take 20 minutes to several hours to complete. These processes also depend on the competence and trustworthiness of field technicians

and devices which introduces another potential point of attack for malware and hackers.

With root keys and a cryptography engine provided in silicon,

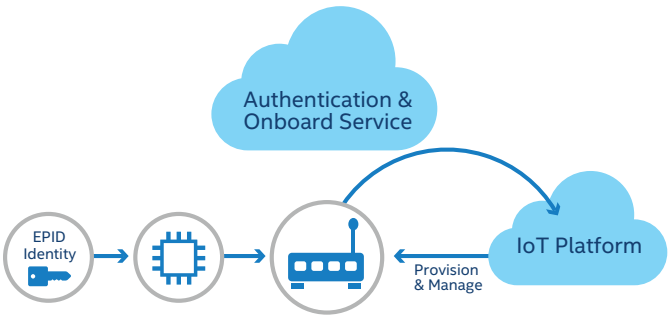

Figure 3. Intel EPID based IoT Onboarding

Intel EPID supports "phone-home" scenarios (See Figure 3) in which a connected device automatically links securely with cloud-based applications for initial authentication, registration, and provisioning. If they choose, centralized deployment teams can also implement their own software-based identity and security solutions on top of Intel EPID during these processes, while retaining the enhanced security provided by the hardware root of trust. With this automated and remote approach, field costs can be significantly reduced and a number of security gaps are closed.

Financial Transaction Security

Mobile and unmanned Point of Sale (POS) devices represent a key use case for emerging IoT technologies, yet they also offer a particularly compelling target for hackers and malware. Intel® Data Protection Technology for Transactions combines Intel EPID-based hardware authentication with end-to-end data encryption. From the instant a transaction is initiated, sensitive data is encrypted and only shared with authenticated devices and applications. Unencrypted data is only processed in a protected execution environment that is isolated both physically and logically from the applications, operating system, and memory of the POS device.

This solution not only provides high levels of security for emerging IoT use cases, but can also provide a needed boost in security for traditional retail settings. It offers an example of the kind of end-to-end security solution that can be built on top of Intel EPID technology. In general, Intel EPID can be used as the basis to securely provision any cryptographic key material over the air or down the wire to provide a flexible, hardware-enhanced foundation for secure interactions.

Connected Cars

The ability of Intel EPID to authenticate devices with or without anonymity offers essential benefits for many IoT use cases. Connected cars are a good example. Suppose a car owner wants to expose real-time data to a trusted mechanic to support predictive maintenance. Knowing the identity of the user and the repair history of the car can help the mechanic provide better guidance. That same car owner might want to share only limited and anonymized data with a traffic monitoring sensor in order to help authorities regulate traffic flow and provide emergency alerts. Intel EPID supports both scenarios, enabling flexible data sharing with privacy tailored to the demands of each use case.

Wearable Healthcare

Healthcare is another area where strong security with tailored privacy offers high value. Suppose a borderline diabetic with a wearable health monitoring device wants to share real-time information with a trusted physician. She would want to share her identity so the physician can provide more accurate medical advice based on her personal health record. That same patient might want to allow a diabetes research team to access some subset of her real-time data, but without divulging her identity. Here again, Intel EPID provides flexible support for both use cases, establishing a common security foundation for both personalized medicine and next-generation medical research (Figure 4).

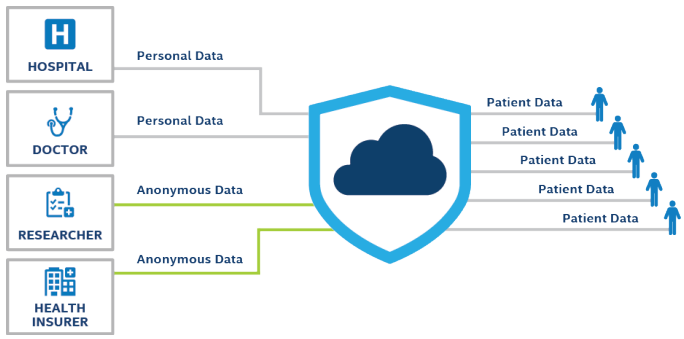

Figure 4. Intel EPID for PHI Privacy

Cost-Effective, Low-Risk Implementation

Security requirements for IoT solutions will vary significantly. In some scenarios, security will have to be uncompromising and cost will not be a primary consideration. In other scenarios, particularly those in which devices and solutions are deployed at massive scale, security will be important, but cost will be equally critical to market success.

Intel EPID is designed to address the full range of IoT security requirements by providing an industry-standard identity solution that is broadly interoperable, proven at massive scale, and can be deployed quickly, affordably, and with a high level of confidence.

Broad Interoperability and a Growing Ecosystem

Intel EPID is supported today in Intel processor-based PCs, laptops, and tablets, in Intel processor-based IoT devices and gateways, and in massive numbers of Intel processor-based servers operating in today's public clouds and enterprise data centers. This wide-ranging support can help to ease implementation for new IoT solutions, greatly increasing the likelihood that a preferred cloud service provider will support Intel EPID-based identity solutions. Even those CSPs that don't yet provide such services can be expected to have the hardware foundation in place and will only need to add appropriate software and procedures.

To help take Intel EPID adoption to the next level, Intel has contributed Intel EPID technology to leading industry organizations for certification. As a result, Intel EPID is now:

- An International Standards Organization standard for identity and privacy (ISO/IEC 20008, 20009)
- A Trusted Computing Group (TCG) standard for attestation.

Intel has also made Intel EPID technology available to processor, microcontroller, and device manufacturers as open source under the Apache 2 license. In mid-2015, Intel jointly announced the licensing of Intel EPID to Microchip and Atmel. At the Intel Developer Forum 2016, a Microchip microcontroller and Dell gateway demonstrated an Intel EPID based onboarding to Microsoft's Azure IoT Hub where the devices powered on and phone home to their owners in the cloud.

Intel is currently working with leading cloud service providers and with IoT hardware and software vendors to help them fully enable Intel EPID in their current and future offerings. The goal is to make Intel EPID a ubiquitous foundation for implementing strong, end-to-end identity and security solutions throughout the IoT.

Proven at Massive Scale

Intel EPID has been proven at scale and across a wide range of use cases. It has been integrated into Intel chipsets since 2008, into Intel processors and platforms since 2011, and is included today in Intel® Core™ processors, Intel® Core vPro™ processors, Intel® Xeon® processors, and some Intel® Atom SOCs.

Intel has used Intel EPID to support security-hardened firmware updates, multi-factor authentication using Intel® Identity Protection Technology, platform trust verification using Intel® Trusted Execution Technology, and digital rights management (DRM) for communications service providers. Altogether, more than 2.5 billion Intel EPID certificates have been generated through Intel fabrication plants and the Intel Key Generation Facility (iKGF).

A Strong Roadmap for the Future

Intel is focused on making Intel EPID the identity solution of choice across the full range of IoT implementations. These efforts include:

- Engagements with leading IoT silicon and device manufacturers to help them integrate Intel EPID into their next-generation products, so Intel EPID is even more widely available to IoT developers.
- Ongoing enhancement to Intel EPID silicon and software to add functionality and simplify implementation, while increasing performance and energy-efficiency.
- Integrating Intel EPID into an increasing variety of Intel processors and SOCs, including high-density, low-power solutions that are specifically optimized for IoT use cases.
- Optimizing Intel key generation services to support today's and tomorrow's massive IoT requirements efficiently and cost-effectively. This may include working with third-parties to help them deliver alternative key generation and certification solutions.
- Ongoing engagements with leaders in the IoT, cloud, and security ecosystems to deliver increasingly secure, comprehensive, and cost-effective security solutions that are optimized for the scale and complexity of the IoT.

Conclusion

There are enormous first mover advantages for organizations developing IoT solutions today. There are also major risks in building solutions in an emerging industry that has yet to establish clear standards. With its proven scale, large existing footprint, standards-based technology, and open source software support, Intel EPID offers a low cost, low risk foundation for building IoT security solutions that are adaptable, easy to implement, and massively scalable.

Intel's extensive efforts with leading IoT and cloud vendors will help to lower risk even more, providing a clear path forward in an otherwise fragmented field of identity and security technologies for the IoT. Given the proven dangers of our increasingly connected world, security must be a top consideration in every IoT implementation. Intel EPID provides a cost-effective foundation that can help the industry move forward more quickly and with greater confidence.

More Information

- To request Intel engagement on Intel EPID or to join our Zero Touch Onboarding POC email- iotonboarding@intel.com
- Intel EPID technical white paper: "Enhanced Privacy ID from Bilinear Pairing," by Ernie Brickell and Jiangtao Li, Intel Corporation. https://eprint.iacr.org/2009/095.pdf
- Platform Embedded Security Technology Revealed: Safeguarding the Future of Computing with Intel Embedded Security and Management Engine (see Chapter 5), by Xiaoyu Ruan, Apress Media, LLC, 2014, available for purchase at http://www.apress.com/9781430265719
- Download the Intel EPID Open Source SDK - https://01.org/epid-sdk

For more information about ISO/IEC 2008, visit http://www.iso.org/iso/catalogue_detail.htm?csnumber=57018 For more information about ISO/IEC 2009, visit http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=57079

 Printed in USA 09/16/DB/DCC/PDF ♻ Please Recycle 0916/DB/ISD/IDF 00000-001US