# Security for Intelligent, Connected IoT Edge Nodes

## White Paper

Eustace Asanghanwa and Ronald Ih
Security ICs, CryptoAuthentication Marketing

The Internet of Things (IoT) reflects one of the biggest technology waves to pass over in a couple of decades. With forecasts of as many as 50 billion connected devices in 2020, it has the potential to touch everything around us. The IoT will span industrial, commercial, medical, automotive, and other applications with consumer implementations having the potential to affect billions of people. Given the scope of individuals, institutions, and systems affected, security has risen to the top of the heap as a critical component in any IoT system, and it's now widely recognized that any serious commercial IoT venture must include security for it to truly take hold.

## Introduction

In assessing IoT network vulnerability, developers have zeroed in on the most fundamental elements — *the edge nodes*. Otherwise known as the “Things” in the Internet of Things, they are the many sensors and actuators that provide the data for the IoT and carry instructions out from the Cloud or a user interacting via a computer, cell phone, in-car system, smart appliance, or other platform.

Edge nodes are usually small, low-cost intelligent devices, but with very limited resources. They are often incorrectly believed to have limited vulnerability to attack. While the servers they talk to and the networks that connect them have well-established security technologies, the edge nodes typically don’t; at least not yet.

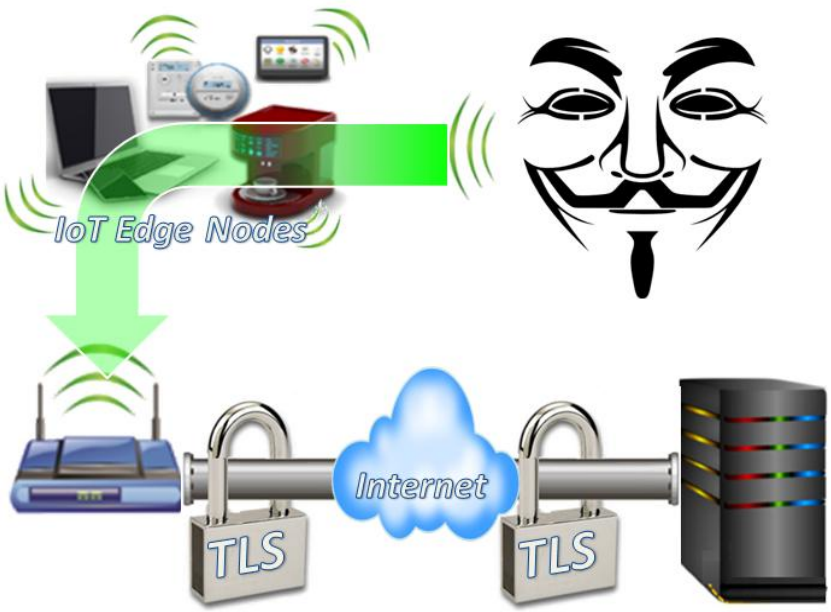
When it comes to securing such systems, people often equate “encryption” with the term “security” when in fact that is only a piece of the security puzzle. One of the first things that must be done to create a secure environment is to reliably discover and prove the *identity* of elements that are connected to your network. You must first determine *who* it is that wants to connect to the network, because without establishing a secure authenticated identity up front, the only thing encryption and Transport Layer Security (e.g. SSL/TLS) can do is protect someone who is not supposed to be on your network to begin with.

To get a better feeling for node security, let’s look at logging into your online bank account as an analogy. You first set up a secure (i.e. encrypted and authenticated) connection between your computer and the bank’s website (which is an https link). However, this secure link does not authenticate you — it only authenticates your computer while creating an encrypted communication channel between your computer and the bank. At this point, the bank does not know you from an imposter. That is where your password comes in. Your password is your cryptographic key, so in theory, only you and the bank know your password. Once you send it to the bank, it compares that to your password it has stored. If they match, then as far as the bank is concerned, you are proven to be who you say you are. From this example you can see that online banking security is provided in two layers:

- The transport layer that sets up the secure connection.
- The application layer that proves (authenticates) your identity via your password.

Similarly, IoT node security must also be multi-layered if the IoT is to be taken seriously.

**Figure 1. Despite a Secure Channel, Attackers Can Access Through the Nodes**



For IoT nodes, TLS is also used to create a secure connection, such as to the cloud. But, to be truly secure, an IoT node must also obtain application layer security. That means that the node itself, and not just the communication channel (i.e. the pipe), should be authenticated. In addition to channel authentication, encryption and data integrity should be established at the application layer to protect the data flowing through the pipe.

With that in mind, IoT devices are now bringing a new paradigm to network connectivity because these devices are often very small and simple with little or no human interaction involved in their operation. And the questions that typically come up cover the gamut. On the one hand, worries about the security of the infrastructure causes people to ask, “How do you know that an IoT device is trustworthy? How do you know that something that is connected to your network is even an IoT device at all, and not a malicious device pretending to be an IoT node?” This is countered with practical questions such as, “What’s the big deal if someone knows what temperature setting my thermostat is set to?” “Who cares if someone knows my lights are on?” “Who cares if someone knows how many steps are logged in my pedometer?”

If you begin to consider not only what data is on the device, but what that device has access to beyond itself on the network, then the issue becomes more substantive. Several high-profile data breaches were accomplished by spoofing the identity of unsecured network nodes, and malicious entities were able to get onto companies’ networks by pretending to be an IoT node. Once on the inside of the network, security becomes much weaker, and they were able to eventually gain access to their victims’ customer database and damage industrial processes. If you consider that this is in addition to accessing cloud services and potentially being able to access and control operation of the nodes themselves, confirming node identity (authentication) becomes a critically important consideration.

While existing Internet security technologies like SSL/TLS can do a good job protecting communications channels between an uncompromised edge node and a server, it’s not invincible. And it does nothing to protect against attacks that don’t involve the incoming network. It should be easy to see that SSL/TLS does not help if an attacker takes control of an edge node.

Tight security involves three fundamental elements, which we refer to by the acronym “CIA”:

- **Confidentiality –** data, whether stored or in transit in a message, should be visible only by authorized persons;
- **Integrity –** a message sent should not change on its way to its destination; and
- **Authenticity –** one needs confidence that the sender of a message is who they say they are.

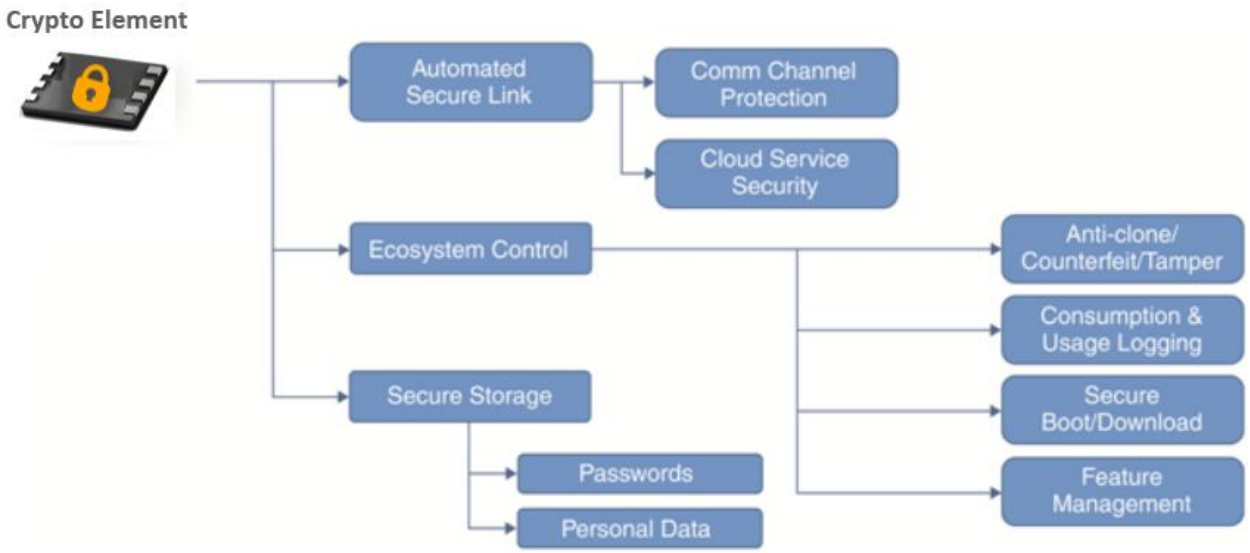
Different technologies contribute to these elements, but common among them is the use of secret or private keys that serve as part of a unique, verifiable identification tag. How those keys are managed – their storage and communication – determines the security of a system.

The challenge is to implement edge node security while remaining within the narrow limits of available computing, memory, and power resources, as well as within budget. The purpose of this paper is to identify critical security strategies for edge nodes, to illustrate the central role keys play in any security solution, and to outline successful key management techniques.

## Secure Identity Cascade Benefits

Once a node or device is established as “trusted,” a myriad of other benefits can become fully realized. These include secure communications, ecosystem control, and secure storage.

**Figure 2. Numerous benefits become available to a node whose identity has been verified**




Once you can verify that an IoT device is what it claims to be, then you can reap benefits only available in a trusted, secure environment.

## Edge-Node Vulnerabilities: What Could Possibly Go Wrong?

Before discussing solutions, we need a better picture of what the vulnerabilities are so that we can provide effective protections. There are two aspects to this: identifying ways that an attacker can compromise the node, and understanding the consequences of such action.

### Attack Modes

There are four ways to get into an edge node:

- Through the network
- Through external ports
- Through proximity attacks (also referred to as “side-channel attacks”)
- Breaking into the device

#### Network Attack

While the network is the best protected port, it is only as good as the security in place. Completely unprotected nodes can no longer survive by hoping to remain under the radar. Web tools like Shodan[1] can crawl the network, identifying every unprotected node. While TLS protection can make a huge difference, subtle vulnerabilities may remain due to bugs in the edge node’s TLS implementation, poor random number usage in crypto algorithms, undetected malware, aggressive protocol attacks by determined experts, and even by weaknesses in the protocols themselves as illustrated by the recently identified FREAK[2] attack.

Even with a perfectly protected network, an attacker might compromise a poorly defended edge node by faking a firmware update and replacing the legitimate code with code written by the attacker.

### Port Attack

The network port (wired or wireless) may be the only connection available on a small, bare-bones edge node. Sophisticated edge nodes, however, may have module ports for plugging in different sensors, or they may have USB or other ports – even wireless ports – for accessories, consumables (like ink cartridges), or test and debug equipment. Each of these ports provides an opportunity to access the edge node. An attack could come through an unused port, or an accessory could be removed and replaced by some other hardware designed to implement an attack. Unlike the network port, there is no established standard for protecting these ports.

### Proximity Attack

Sophisticated attacks can also occur without making any connection to the edge node. By tapping the power line or measuring emissions or vibrations on an unprotected device, it's possible to extract information about the keys. By exploiting undocumented behaviors or faults – like issuing a power surge – it may be possible to put a device into an undocumented, unsecured state.

### Physical Attack

Finally, a determined attacker may physically disassemble the edge node in an attempt to probe internal circuits (with or without power), or even remove and deprocess ICs to learn the contents of embedded memories.

Comprehensive security must protect against all of these modes of attack.

## Consequences

Of course, we lock only those things we think contain valuables. It might seem that a simple sensor node would be of limited value to an attacker, but the consequences of a successful attack can put an entire network, and anything connected to that network, at risk.

By breaking into the edge node, even through a network security weakness, the attacker may get access to all of the secrets that the security is supposed to protect – and in particular, the keys needed to implement security. Once the keys are taken, then all other security protections can be defeated – including encryption and message authentication.

Once an attacker has control of the edge node, he or she can change the behavior of the node on the network without alerting the network that anything is wrong. As far as the other servers are concerned, the edge node is still a "trusted" entity, so secrets are willingly divulged without any realization that they've falling into the wrong hands.

Loss of such secrets can undermine customers' confidence that their financial, medical, identity, and other data are private and secure. It may also violate regulations, whether (in the US) the FTC for trade issues, HIPAA/FDA for healthcare applications, or the SEC/FDIC for financial transactions. Attacks on some networks such as air control and road traffic systems, the electrical grid, airplanes, and automobiles may also affect public safety, and industrial operations may become unreliable, if not outright unsafe.

## The Right Way to Protect an Edge Node

We've seen some of the many ways edge nodes can be compromised. The following measures, all of which involve key storage in one way or another, will ensure that such attacks can be thwarted. While there are never 100% guarantees with security, these measures offer the best possible protection, and they ensure that an attacker has no way of determining critical system keys. These approaches each support the important elements of CIA:

- **Authenticity** – Prove the identity of any visitors coming in over the network.
- **Authenticity** – Authenticate any accessories that try to attach to the node. ()
- **Confidentiality** – Encrypt messages.
- **Integrity** – Append a Message Authentication Code (MAC) to all messages to prove that no one has altered the message en route.

In addition, steps can be taken to protect from "proximity" or "side channel" attacks. These are practical in nature and can be implemented on the entire system, or just on a key subsystem.

- Store keys in protected hardware so that there is no electrical access to the key.
- Shield the system to prevent electromagnetic emissions from divulging key information.
- Add circuitry specifically to confound attempts to monitor power or other signals. This may include dummy counters or circuits with some element of randomness to scramble useful information.
- Encrypt the key in storage. Even though the key may be electrically inaccessible, a determined attacker may try to strip away layers of the device to see into embedded FLASH memory and retrieve the key that way. Encryption neutralizes this attack.
- Eliminate extraneous ports. It may seem useful, for instance, to include a debug port, but if the likelihood is that it will never be used, then your system will be more secure without it.

It's also critically important to protect keys during the entire manufacturing process. A well-thought out scheme that keeps secret keys secret from their generation to insertion into the key storage device is necessary. The use of hardware security modules (HSMs) that store the keys in encrypted format and in protected hardware is an excellent and proven methodology.

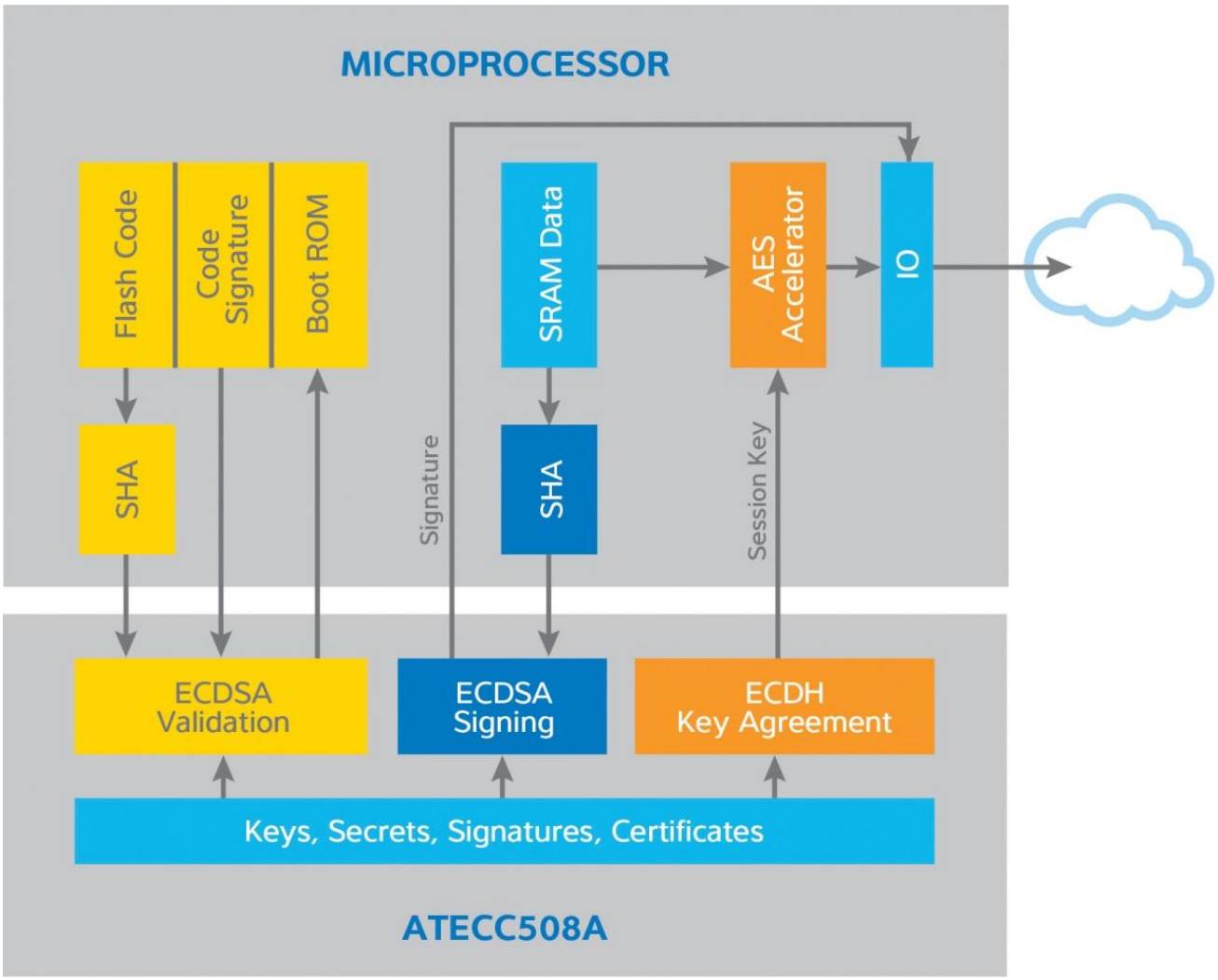
## Real Solutions for Protecting Keys

Atmel provides a range of cryptographic solutions in the form of crypto element devices[3]. Because these devices act as hardware crypto accelerators, the focus is often on their usefulness for offloading complex mathematics from the host processor. But there's an even more important aspect: cryptographic operations involve keys, so they must be stored in well-hidden, protected hardware that ensures that the keys will never be visible in the way they would be if you tried to do the same calculations in software or in unprotected hardware.

The newest Atmel ATECC508A CryptoAuthentication™ crypto element is an ECC-based device that includes ECDH[4] key agreement has built-in ECDSA[5] based asymmetric authentication capabilities, and features protected hardware-based secure key storage, which is the strongest there is.

The ATECC508A is adapted perfectly for securing IoT edge nodes since it has both ECDSA and ECDH. Adding a tiny ATECC508A to any system with a microcontroller, including IoT nodes, easily and efficiently brings confidentiality, integrity, and authentication to that system.

**Figure 3. ATECC508A Works Alongside Any Microprocessor to Securely Provide Confidentiality, Data Integrity, and Authenticity**




The ATECC508A can be added alongside any microcontroller at very little cost. Single-wire or $I^2C$ connections minimize pin count, and package options can be as small as 2mm x 3mm. Power consumption is extremely low with sleep current at less than 150nA.

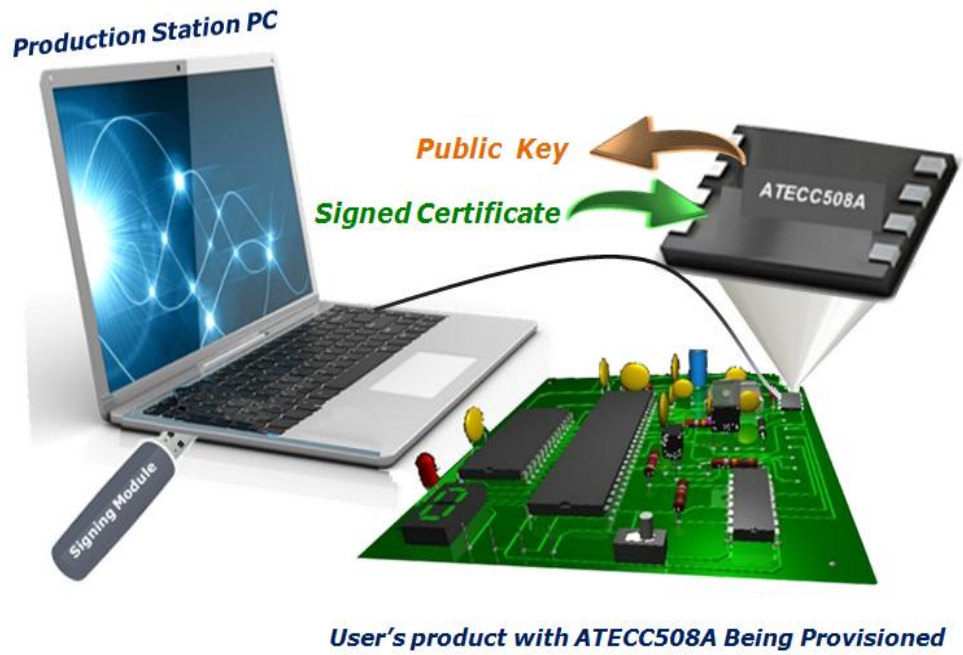
Crypto elements execute algorithms internally, taking inputs provided by the processor and returning the calculated results (i.e. signature, authentication, session keys, etc.) without revealing the means of that calculation. A high-quality True Random Number Generator (TRNG) helps prevent a transaction from ever being replayed successfully. An internal serial number helps to ensure key uniqueness, and high capacity counters are provided to track authentications.

Physical and cryptographic countermeasures make it impossible for an attacker to sniff operations to learn the keys, or probe the device to obtain the keys.

- The entire device is shielded with a serpentine metal pattern that prevents internal signal emissions from being detectable outside and provides a visual barrier against someone opening the package to observe and probe operations. The shield is electrically connected to the rest of the circuit. If it is compromised, the device will no longer operate, preventing a determined attacker from probing circuit nodes to learn the secrets.
- Regulators and counters are used to confound power and signal signatures.
- There are no extra internal pads for test and debug, so opening the package provides no additional access points.

An important benefit of Atmel crypto element devices is the provisioning at production is made very easy by use of simple modules (available from Atmel) that enable secure insertion of secrets and signed certificates into crypto element devices. Provisioning can also be done by Atmel or by the Atmel authorized distributors.

**Figure 4. ATECC508A Provisioning at Production Time**




## Summary

Security is fundamental for the successful rollout of the Internet of Things[6]. Edge nodes are currently the weakest link in ensuring IoT security and the protection of cryptographic keys locks down the edge nodes. The best way to achieve lockdown is by protected hardware. It's the only way to keep those keys and other secrets away from prying eyes. The Atmel CryptoAuthentication™ family of crypto elements provides a rock-solid means of storing keys in protected hardware and managing those keys to achieve multi-layer security. The broad Atmel portfolio of microcontrollers, wireless devices, and crypto elements brings state of the art intelligence, securely connected to the IoT, and beyond.

## References


1. “The Search Engine for the Internet of Things,” Shodan. 2015. www.shodan.io
2. “FREAK,” Wikipedia. September 5, 2015. http://en.wikipedia.org/wiki/FREAK.
3. “Smarter Security For Your Everything, Atmel Has You Covered,” Atmel. 2015. www.atmel.com/Microsite/security/overview.aspx.
4. www.semiwiki.com/forum/content/3966-ecdh-key-exchange-practical-magic.html. “ECDH Key Exchange is Practical Magic,” SemiWiki.com, Bill Boldt. October 28, 2014.
5. “The ABCs of ECDSA,” Atmel, William Boldt. August 6, 2014. http://blog.atmel.com/2014/08/06/the-abcs-of-ecdsa-part-1/.
6. “Is the Internet of Things Just a Toy?” Atmel, William Boldt. January 2, 2015. http://blog.atmel.com/2015/01/02/is-the-internet-of-things-just-a-toy/


## Editor’s Notes About Atmel Corporation

Atmel Corporation (NASDAQ: ATML) is a worldwide leader in the design and manufacture of microcontrollers, capacitive touch solutions, advanced logic, mixed-signal, nonvolatile memory and radio frequency (RF) components. Leveraging one of the industry's broadest intellectual property (IP) technology portfolios, Atmel® provides the electronics industry with complete system solutions focused on industrial, consumer, security, communications, computing and automotive markets.

Today, microcontrollers are just about everywhere, powering an expansive array of digital devices. Many are calling this the era of The Internet of Things, a highly intelligent, connected world where Internet-enabled devices will outnumber people. Atmel is pleased to be at the heart of this movement, developing innovative technologies that fuel machine-to-machine (M2M) communication and the “industrial Internet.”

Further information can be obtained from the Atmel website at www.atmel.com.


Contact: **Eustace Asanghanwa**, Security ICs, CryptoAuthentication Marketing
Tel: (+1) (719) 540-6689
eustace.asanghanwa@atmel.com
1150 E Cheyenne Blvd
Colorado Springs, CO 80906, USA

**Ron Ih**, Crypto Marketing, Security ICs, CryptoAuthentication Marketing
Tel: (+1) (408) 437-2018
ronald.Ih@atmel.com
1600 Technology Dr
San Jose, CA 95110, USA


**Atmel Corporation** 1600 Technology Drive, San Jose, CA 95110 USA **T:** (+1)(408) 441.0311 **F:** (+1)(408) 436.4200 | **www.atmel.com**