Atmel Crypto Athentication™

ATSHA204

V 1.0

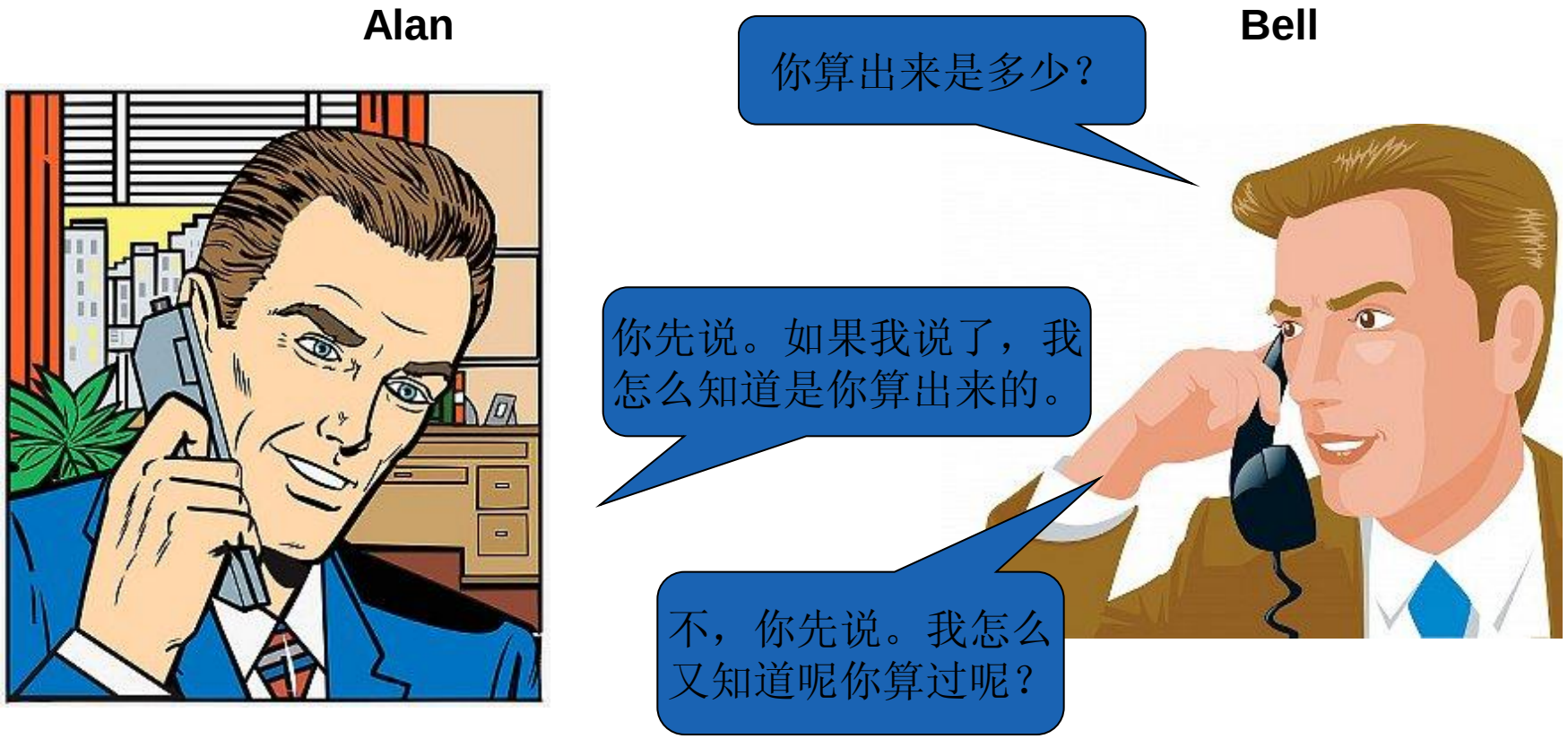
- 什么是加密芯片

  它本身具有十分安全的保密性，内部可以存储秘密数据，内置加密算法，通过安全的认证协议进行认证过程。

- 认证协议的作用

  认证双方在不直接出示密钥的情况下，能够证明自己知道密钥。

散列函数Hash



Alan和Bell都是密码学教授,有一天，他们共同解决一个数学难题。在办公室里他们都没有想出来，却恰好在家里同时想出了答案。

散列函数Hash

- 不可逆的函数

$$c = F(s)$$

知道函数F和c，很难反向运算得s。

例如，F是3的s次方后取前2到6的有效位数，共5位数为c。
随便取一个值，s=286，则3的286次方是
2.86206076306554309658553144254 31e+136
取前2到6的有效数字得，c=86206

$$F(286) = 86206$$

散列函数Hash

把函数结果
告诉我吧。

我运算过后是
86206

恩，我已经知道你是
知道的。你不必说出
答案了。

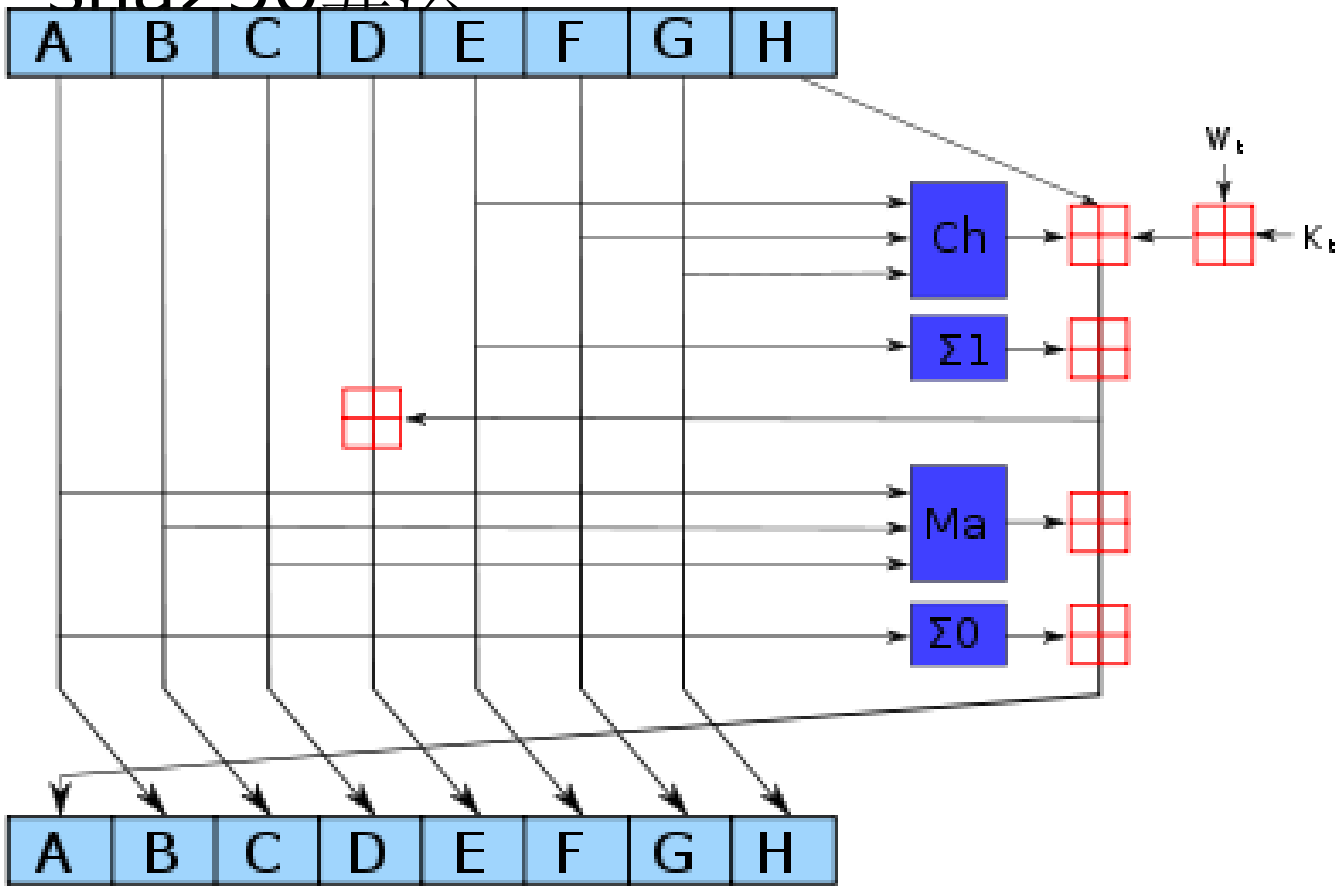
散列函数Hash

SHA家族的五个算法，分别是SHA-1、SHA-224、SHA-256、SHA-384，和SHA-512，由美国国家安全局(NSA)所设计，并由美国国家标准与技术研究院(NIST)发布；是美国的政府标准。
后四者有时并称为SHA-2。

算法	输出散列值长度（bits）	中继散列值长度（bits）	数据区块长度（bits）	最大输入消息长度（bits）	一个Word长度（bits）	循环次数	使用到的操作符	碰撞攻击
SHA-0	160	160	512	$2^{64}-1$	32	80	+,and,or,xor,rotl	是
SHA-1	160	160	512	$2^{64}-1$	32	80	+,and,or,xor,rotl	存在2^{63}的攻击
SHA-256/224	256/224	256	512	$2^{64}-1$	32	64	+,and,or,xor,shr,rotr	尚未出现
SHA-512/384	512/384	512	1024	$2^{128}-1$	64	80	+,and,or,xor,shr,rotr	尚未出现

散列函数Hash

- sha256算法



散列函数Hash

- sha256算法

$$256\text{bit}\_string = SHA256(string\_anylong)$$

SHA256("apple"):
3A7BD3E2360A3D29EEA436FCFB7E44C7
35D117C42D1C1835420B6B9942DD4F1B

SHA256("apple ")(多了一个空格):
E0F6F390C37556B5EB3292A63159AEA8
EC795A4A1D4F22A18ABB14AC7341508F

SHA256("Linux"):
4828E60247C1636F57B7446A314E7F599
C12B53D40061CC851A1442004354FED

散列函数Hash

- Hash算法与加密算法

Hash算法是不可逆的，也就是不能通过输出文本转化回原文本。不同文本经过Hash算法后可能输出相同的结果。

而加密算法是可逆的，每个加密算法都会有相应的解密算法。原文与密文一一对应。

HMAC 挑战响应

- HMAC

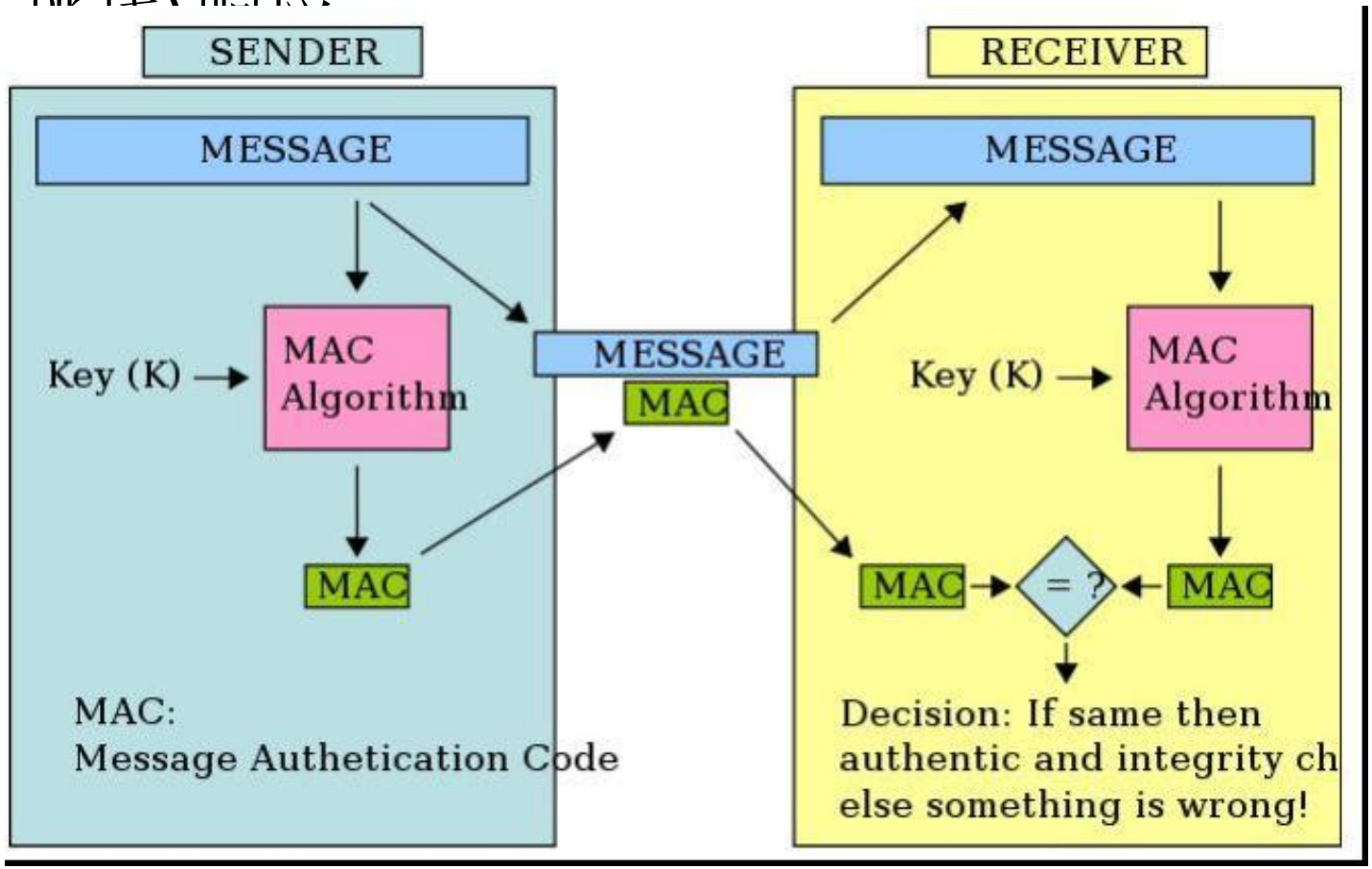
  HMAC是密钥相关的哈希运算消息认证码（Hash-based Message Authentication Code），HMAC运算利用哈希算法，以一个密钥和一个消息为输入，生成一个消息摘要作为输出。

- 挑战\响应

  客户端发送一个消息作为挑战给服务器，服务器使用事先存储好的密钥求MAC，发回客户端，这是响应。客户端根据响应来认证。

HMAC 挑战响应

- 挑战响应



ATSHA204

What can ATSHA204 do?

- Authenticate an Accessory
- Authenticate Firmware
- Securely Exchange Session Keys
- Secret Storage

ATSHA204

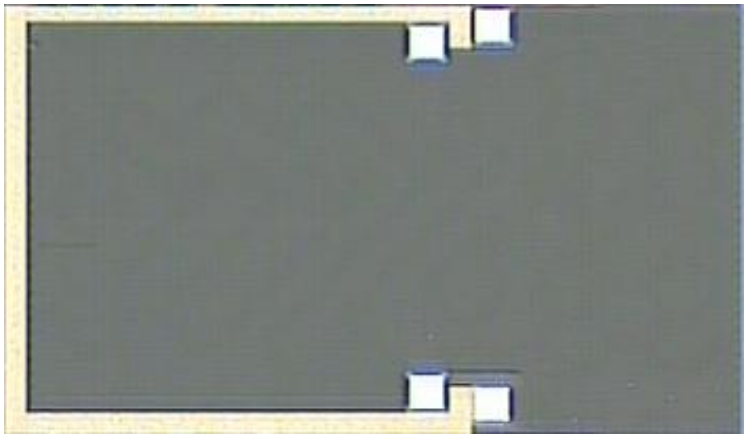
AT88SC0104 vs ATSHA204

	AT88SC0104	ATSHA204
Algorithm	Atmel Algorithm	Public SHA256
Key length	64bit	256bit
Interface	I2C	Single Wire & I2C
Memory	1KB	4KB
NDA requirement	Yes	No

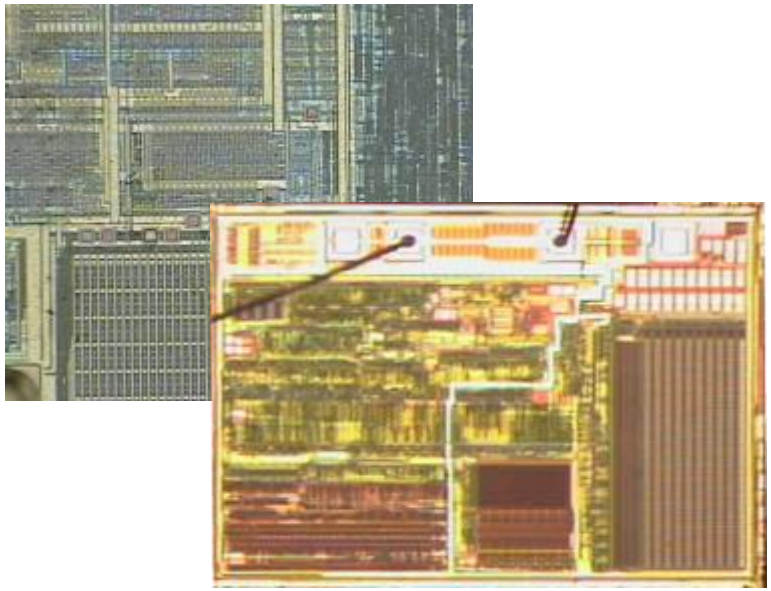
ATSHA204 Security Features

- **Robust Crypto Algorithm**
  - SHA256 MAC, HMAC
- **Advanced Multi-Level HW Security**
  - Active shield over *entire* chip
  - All memories internally encrypted
  - Internal state consistency checking
  - Security protocols hard coded
  - Supply tamper protection
  - Internal clock generation
  - Secure test methods, no JTAG
  - No debug probe points, no test pads
- **Designed to Defend Against:**
  - 'Dumpster-diving' attacks
  - Microprobe attacks
  - Timing attacks
  - Protocol attacks
  - Fault attacks
  - Power cycling
- **Just as Secure as Smart Cards!**

ATMEL



Competitors



ATSHA204

Key

- 256 bits long.
- ATSHA204利用这些key作为HASH消息源的一部分。用于MAC,CheckMac,HMAC, GenDig指令。
- EEPROM的data zone的任意Slot可以存储Key。

(1) Diversified keys根据产品序列码生成key

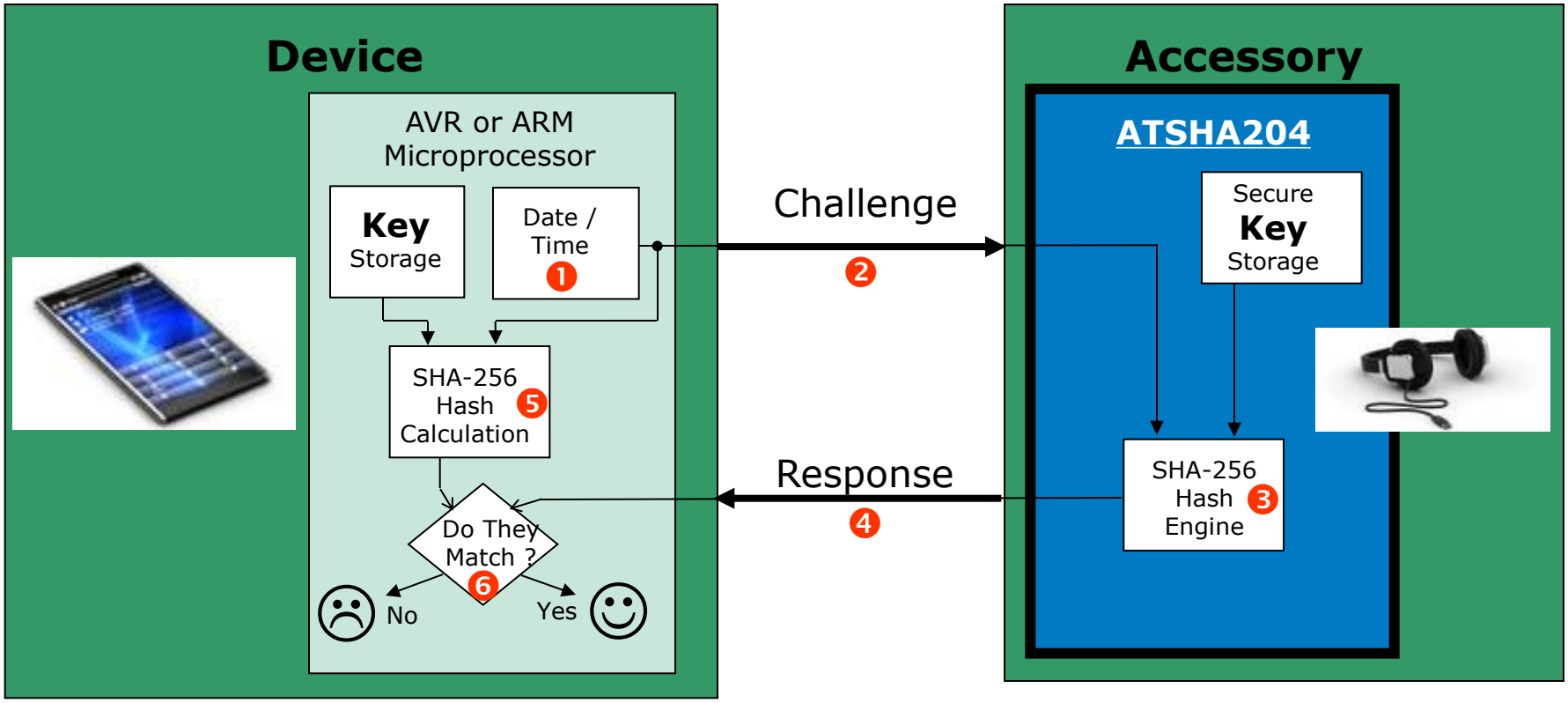
(2) Rolled Keys: 防止每次认证都使用相同的key

(3) Created Keys:根据已知的key产生新的key

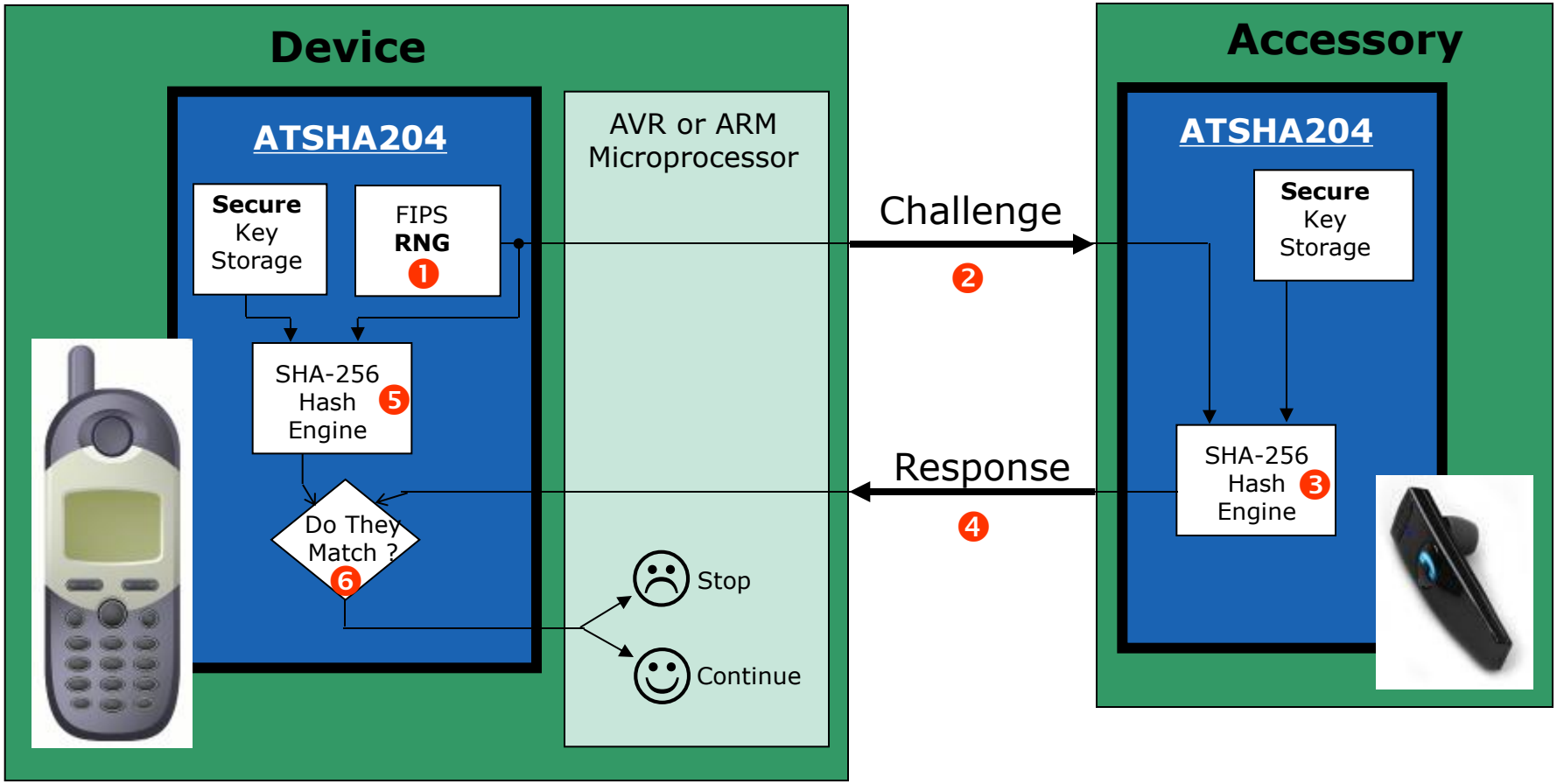
(4) Single-use Keys 使用有次数限制

(5) Password Checking 密码检查

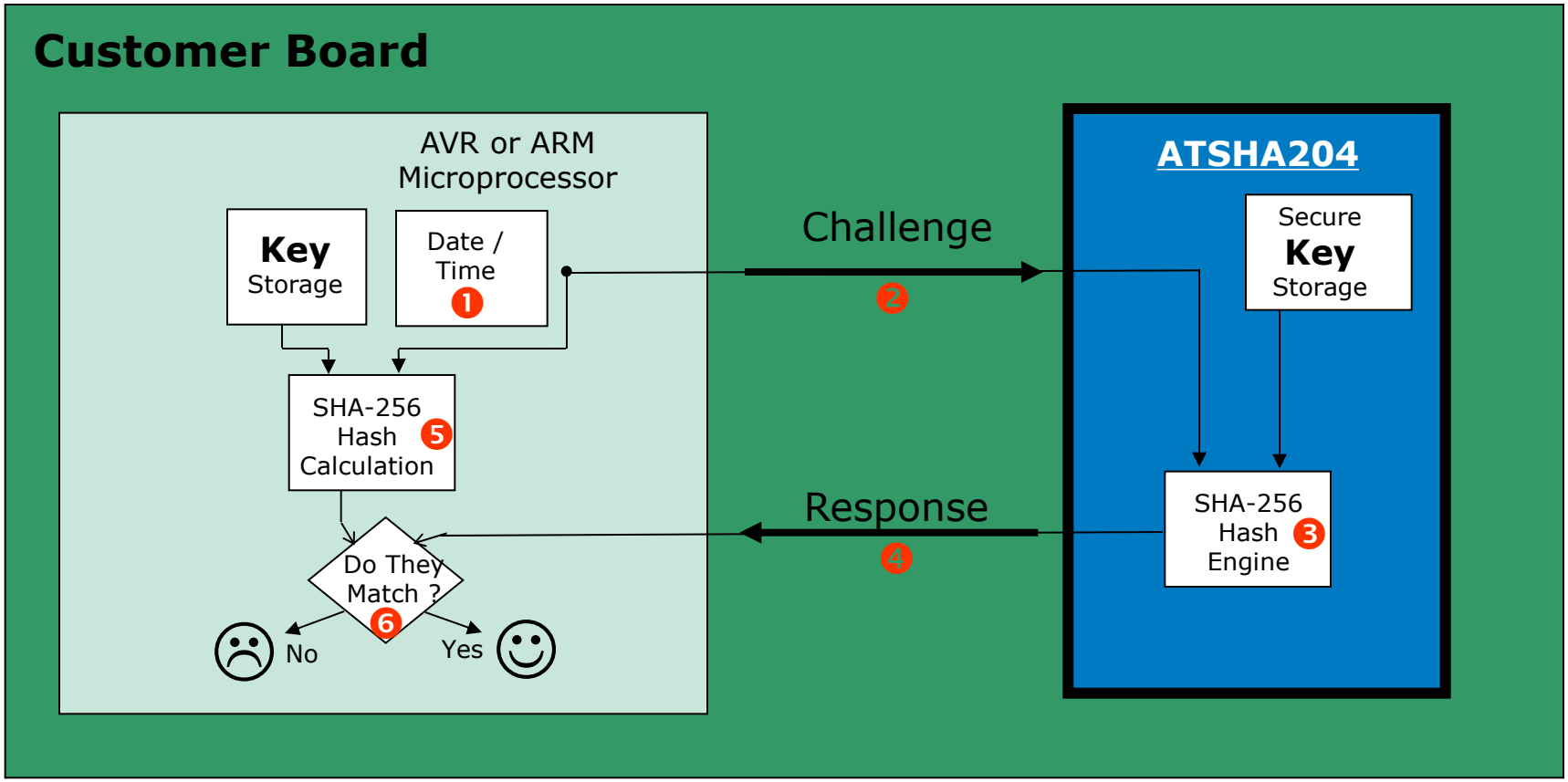
Accessory Authentication



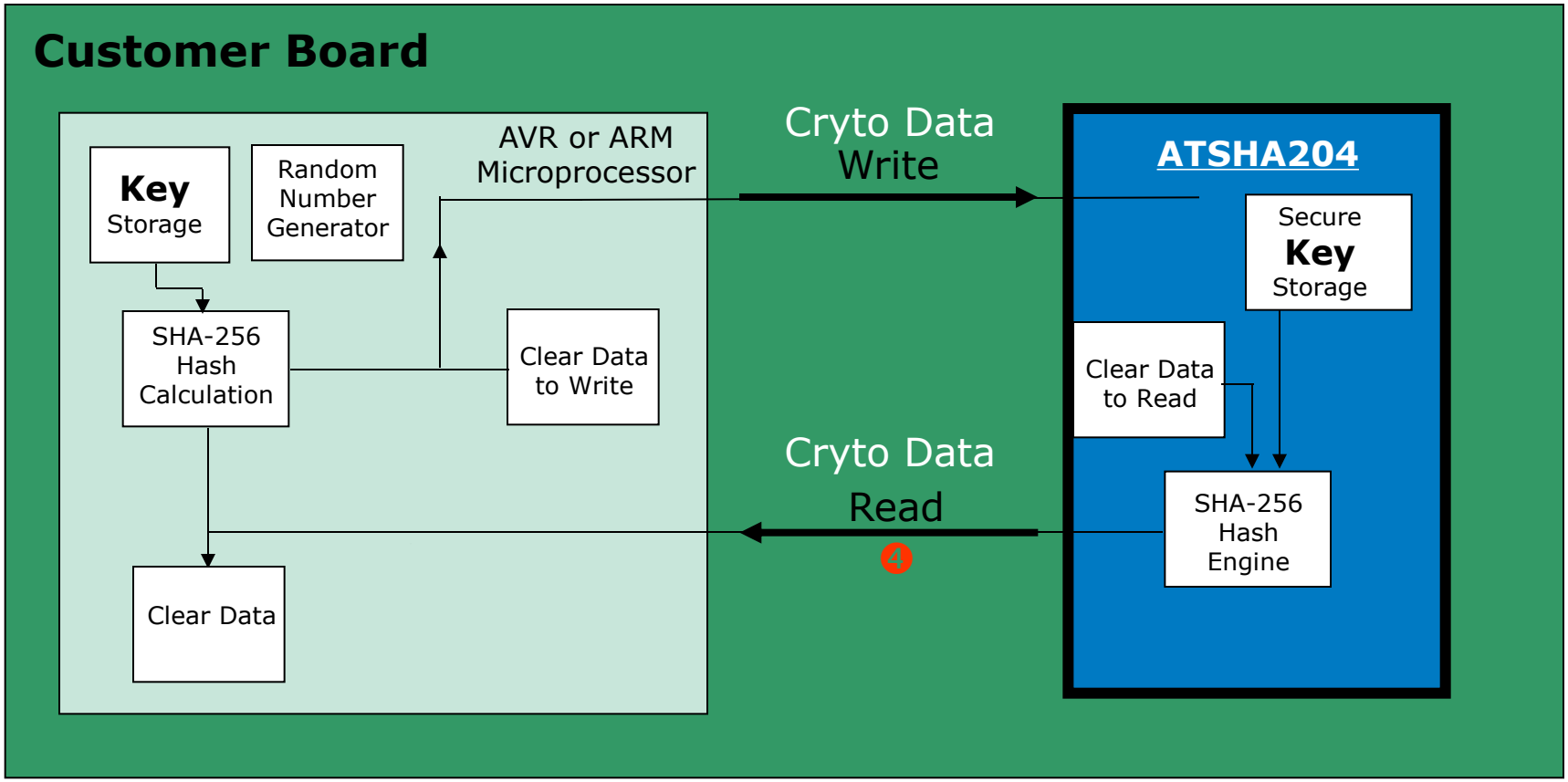
Accessory Authentication – Host Chip



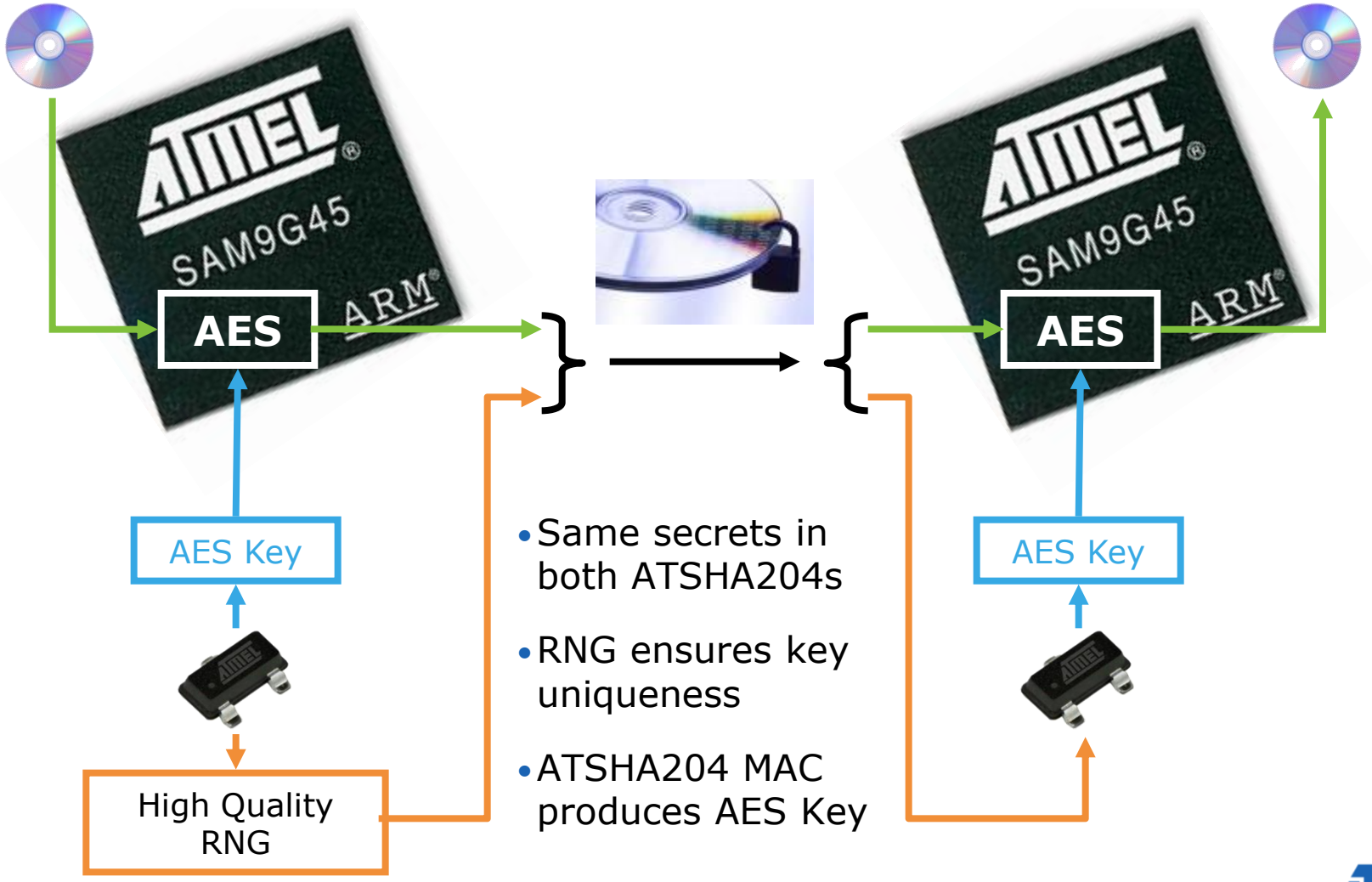
Firmware Authentication



Secret Storage



Session Key Exchange



Mutual Authentication

- Uniformity across entire product lines
- Tools authenticate batteries before allowing use
- Charger Authenticates batteries before charging
- Batteries authenticate charger before charging
- Only valid products can be used together

Managing Subcontractors

- **Chip Limits Subcontractor Actions**
  - Prevent unauthorized overbuilds
    - OEM gives subcontractor limited qty of security devices
  - Warranty Tracking
    - Subcontractor logs mfr date, conditions, etc
  - Personalize chip for use at one subcontractor only
    - Match correct part with equipment/information at that subcon
  - Control model numbers built by particular subcon
    - Subcon only has authentication information for certain models
- **Secure Programming Feature**
  - Protects secrets at third party subcontractors
  - Atmel can securely program parts for high volume customers
- **Customer: "We have more products sold under our name that are not produced by us than what we produce"**

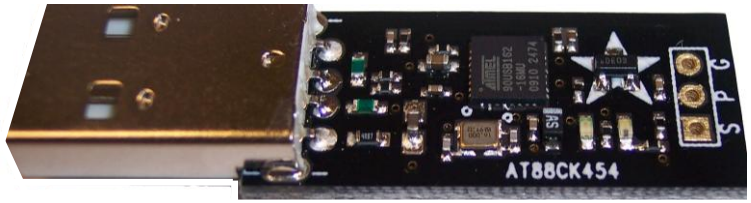
CryptoAuthentication Kits and Support

- **Multiple Demo/Eval/Kit Boards**
  - Modular for compatibility with STK/EVK boards
- **Source Code Library Code**
  - Speed customer development cycle
- **Extensive Documentation**
  - Quick Start and Hardware User Guides
  - Application Notes
- **Demonstration / Evaluation PC Software**
  - Atmel Crypto Evaluation Studio (ACES)

ATSHA204 USB Dongle

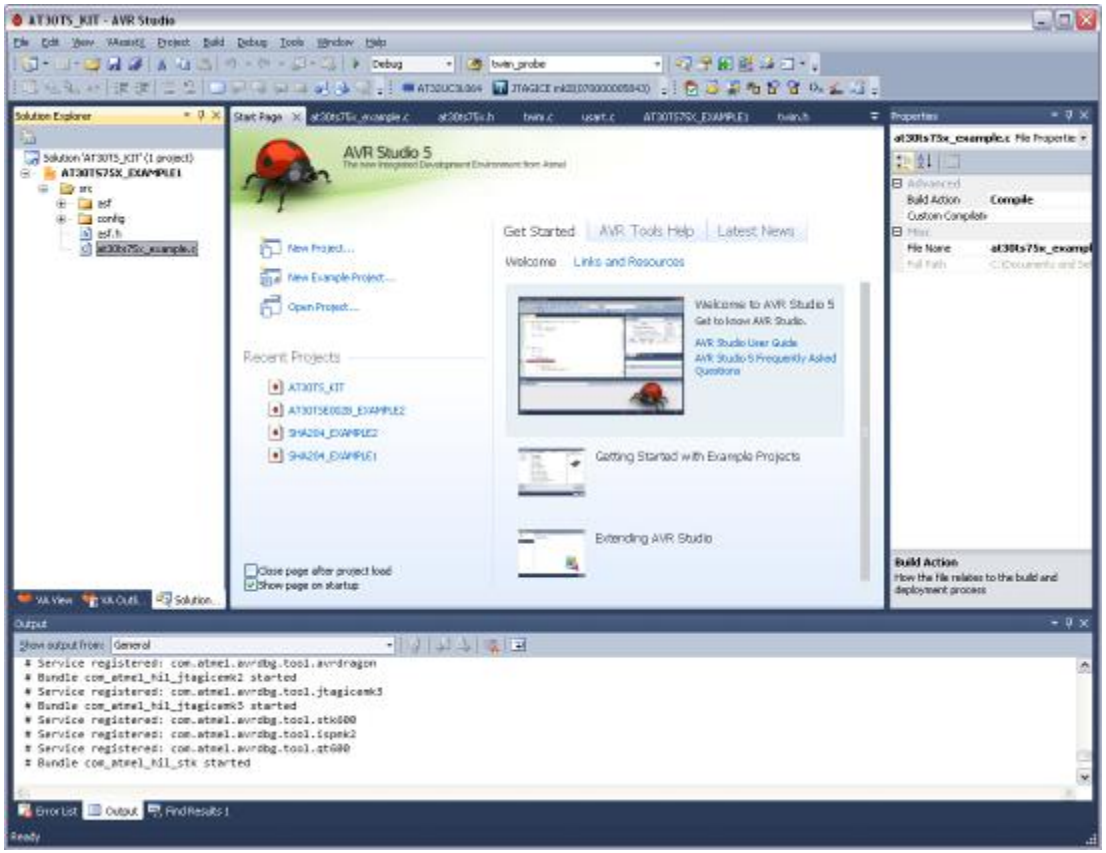
Small and Simple for Quick Demos

- Full PC GUI (ACES) support for device evaluation & experimentation
- Low cost



AVR Studio 5 Integration

- **Source Code Library**
  - Online, no NDA
  - Supports most AVR and ARM devices
  - I2C or Single Wire Intfc
  - SIO, UART or SW GPIO
- **Integrated into ASF framework**

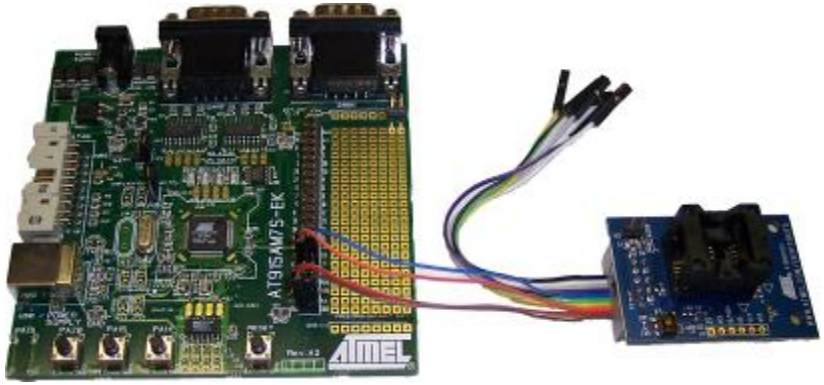


Kits Integrated With Atmel Dev. Tools

- **Pluggable Adapters to STK/EK boards**
  - Sockets to simplify lab prototyping
  - Available for multiple package types
  - Single or Dual chip for Host/Client development
- **Source Code Library Online**
  - Fully integrated into ASF framework

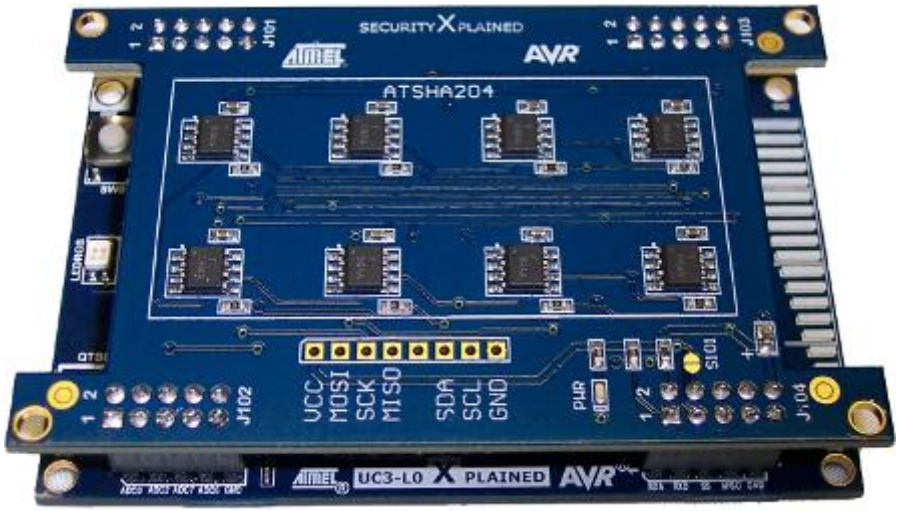
AT88CK101

STK600



SAM7

Xplained Top Board



- **Multiple CryptoAuthentication Chips**
  - Each at different I^2C address
  - Program/experiment, switch to next to experiment with different configurations

- **Kit Project to run ACES GUI**
  - Online download for AVR

ACES PC Software Tool

- **Demonstrate, Evaluate & Configure**