SAND2009-1407P

Intrinsic Code Verification

ICV

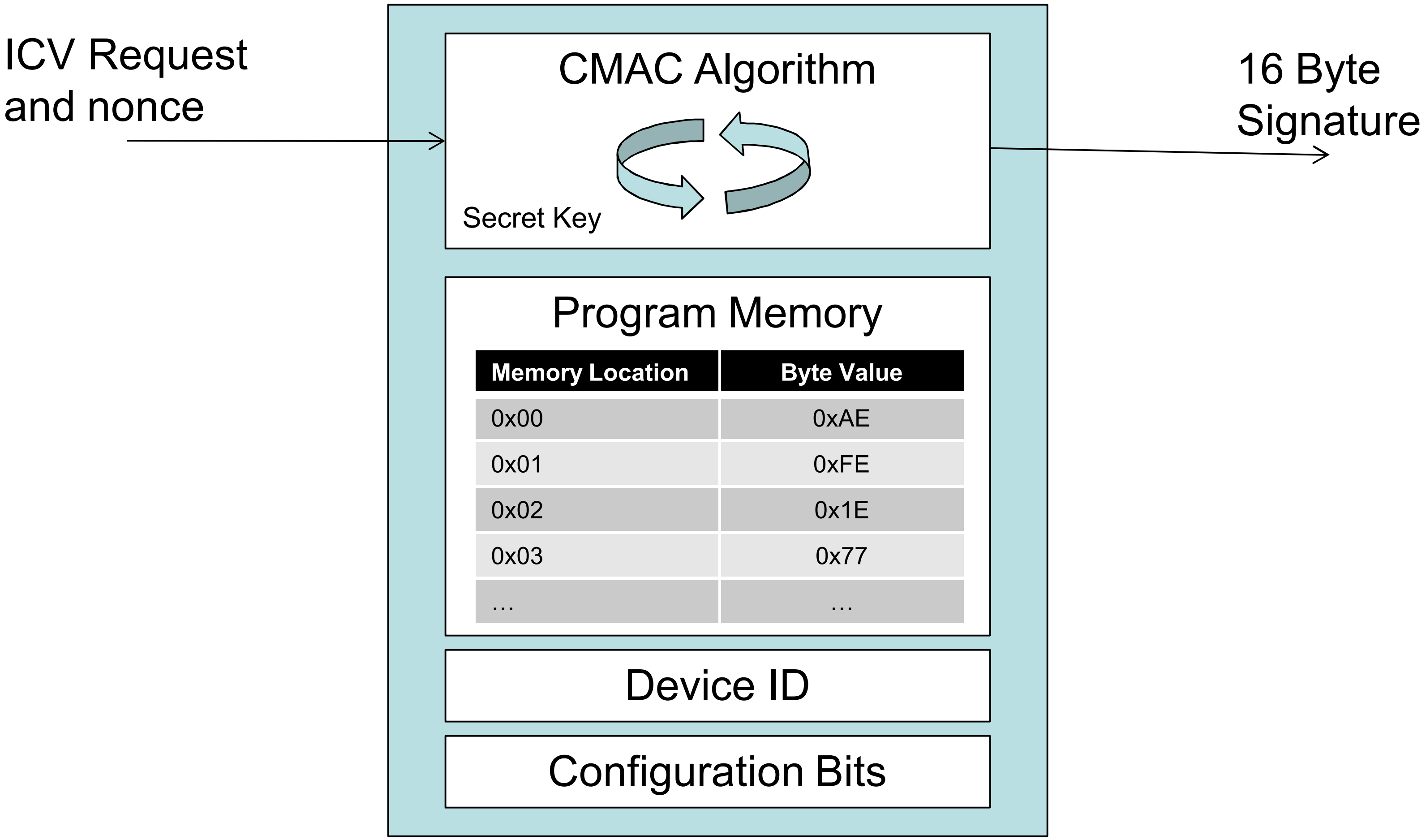
March 12, 2009

Troy Ross
Sandia National Laboratories
Albuquerque, New Mexico, USA
tdross@sandia.gov

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company for the
United States Department of Energy's National Nuclear Security Administration under contract
DE-AC04-94AL85000.

SAND Number: 2008-4434C

ICV Basic Concept



ICV Request and nonce

CMAC Algorithm

Secret Key

16 Byte Signature

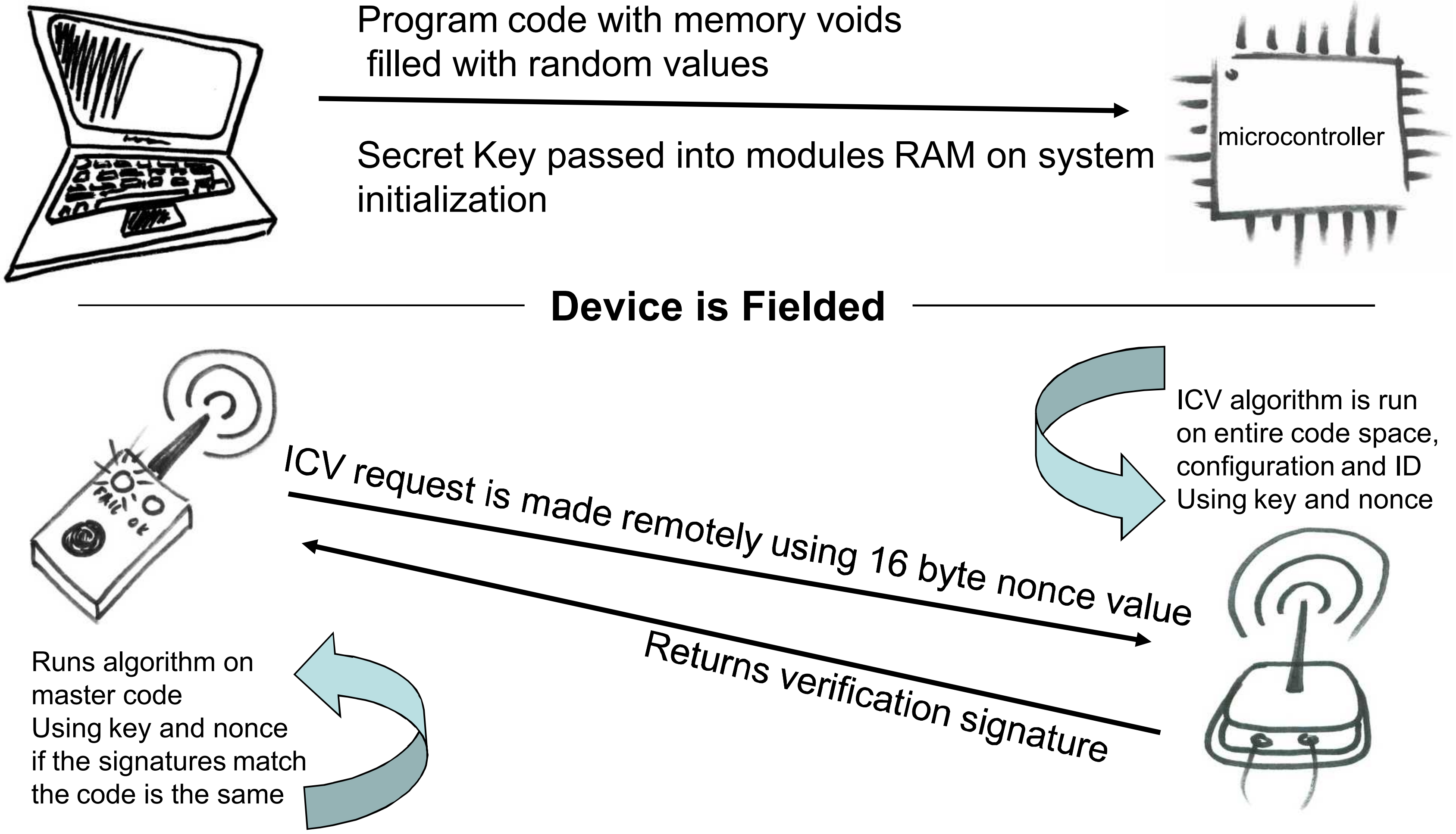
Program Memory

Memory Location	Byte Value
0x00	0xAE
0x01	0xFE
0x02	0x1E
0x03	0x77
…	…

Device ID

Configuration Bits

ICV Basic Concept



Program code with memory voids filled with random values

Secret Key passed into modules RAM on system initialization

Device is Fielded

ICV request is made remotely using 16 byte nonce value

Returns verification signature

ICV algorithm is run on entire code space, configuration and ID Using key and nonce

Runs algorithm on master code
Using key and nonce
if the signatures match the code is the same