DESIGN AUTOMATION & EMBEDDED SYSTEMS

FPGA - EMBEDDED - INTERNET OF THINGS - PCB TECHNOLOGIEËN

29 OKT
1931 CONGRESCENTRUM
BRABANTHALLEN
DEN BOSCH

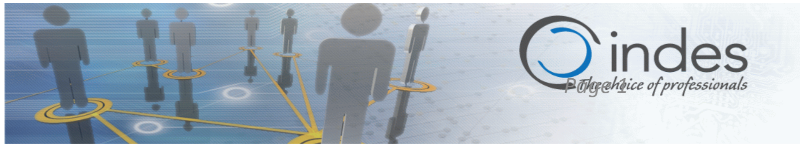
D&E event 2014

Securing the Internet of Things

Gerard Fianen

info@cypherbridge.com

Cypherbridge Systems



INDES-IDS BV - Embedded Software Development

“The choice of professionals”

info@indes.com

www.indes.com/embedded

Tel: 0345 - 545.535

IoT - Growing Pains

- Hacking in embedded control systems is increasing risk

- Securing Personally Identifiable Information (PII) is crucial for the rollout and growth of IoT market

- Regional or National Regulatory requirements such as HIPPA require electronic data privacy layers to protect personal information, and to verify data integrity and authenticity

- Removable flash drives make it easy to install and steal programs or data

Security Protocols and libraries

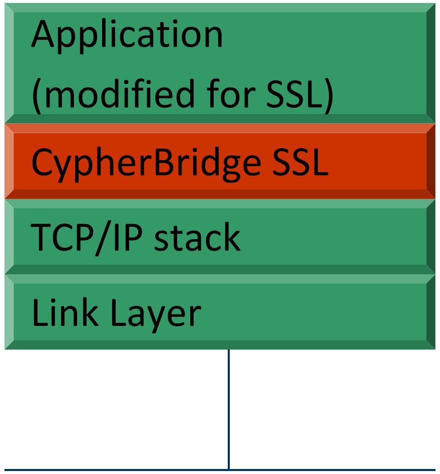
- ✓uSSL/TLS – point to point secure channel above TCP layer. Use this for per-application secure client or server. Flexible protocol for embedded TLS HTTPS, SMTPs, DTLS UDP, etc. Supports secure file transfer by FTPS.

- ✓uSSH – Secure telnet replacement. Supports secure file transfer by SCP

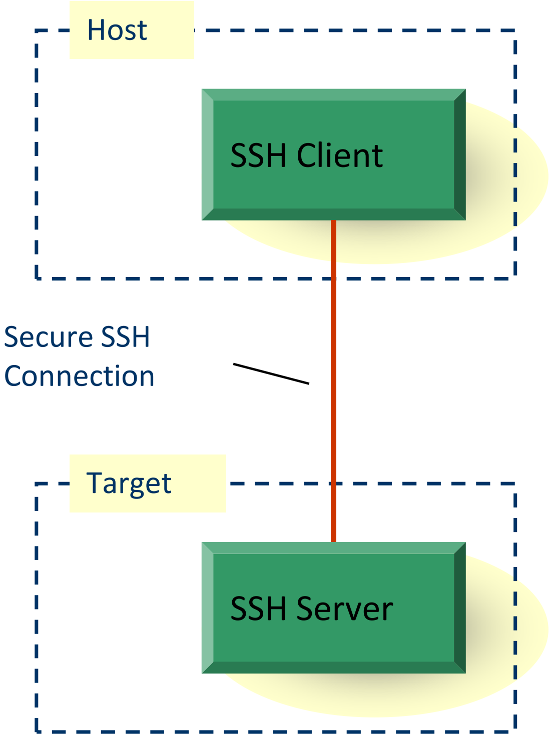
- ✓uVPN – point to point secure channel at IP layer. Bulk encryption for all traffic between endpoints. Use for road warrior or fixed infrastructure connection.

- ✓uFile – Add encrypted file system to protect stored data on embedded system
- ✓uCrypt – general purpose crypto library including high-strength cipher & hash

SSL and SSH



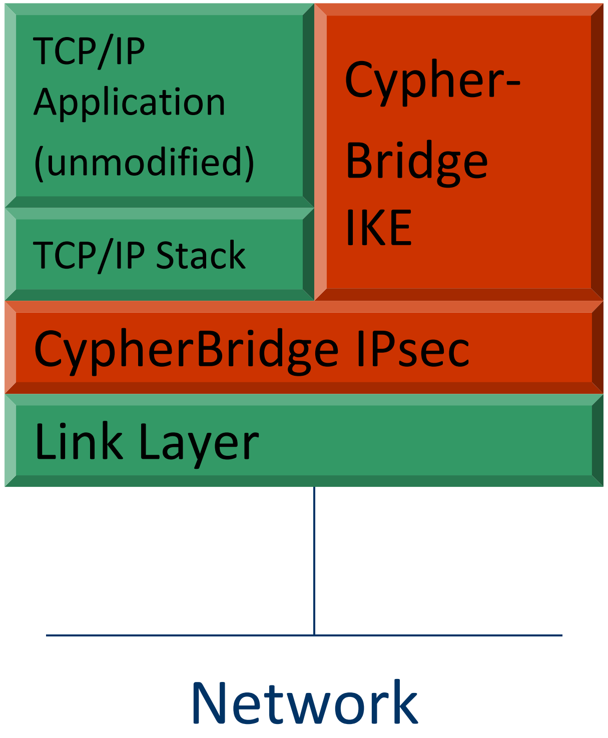
SSL, TLS 1.0, 1.1 and 1.2,
PKI X.509 certificates, crypto,
hashing and network protocols.



SSH and secure TCP/IP tunnel
embedded server and client,
flexible interactive shell, and SCP copy option.

IPSEC

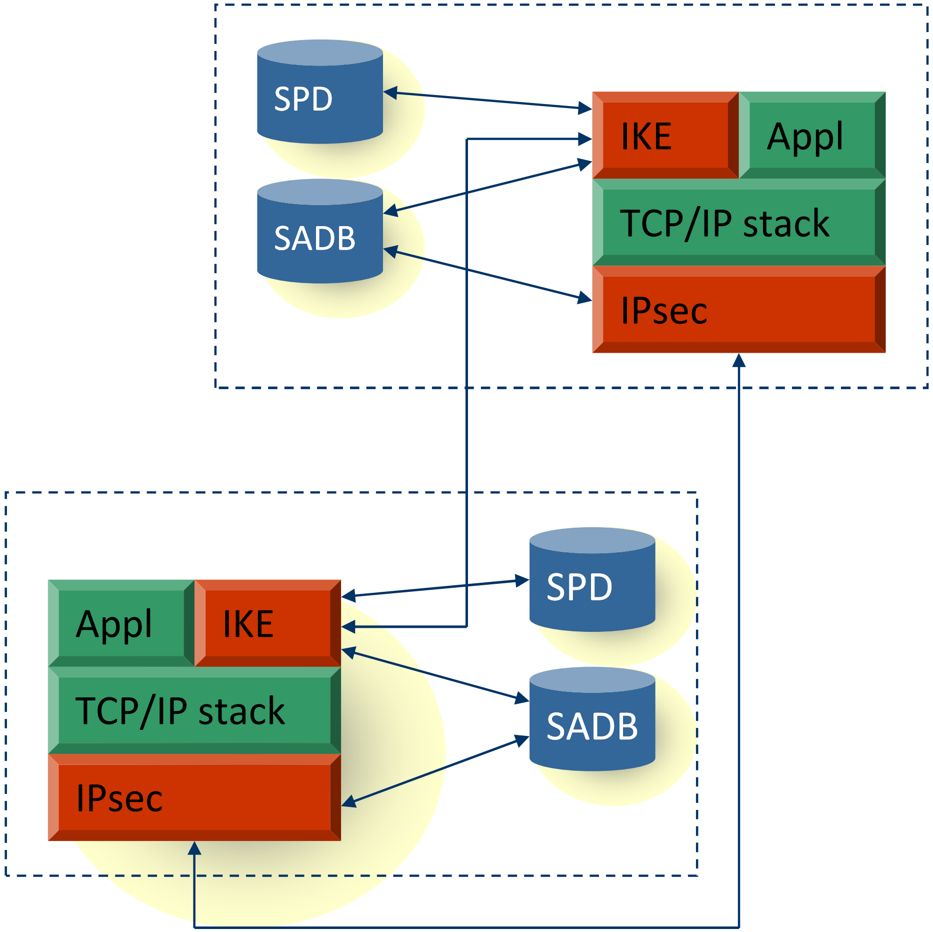
- **Standard IP-protocol not secure**
- **IPsec wil add**
  - **Encryption**
  - **Authentication**



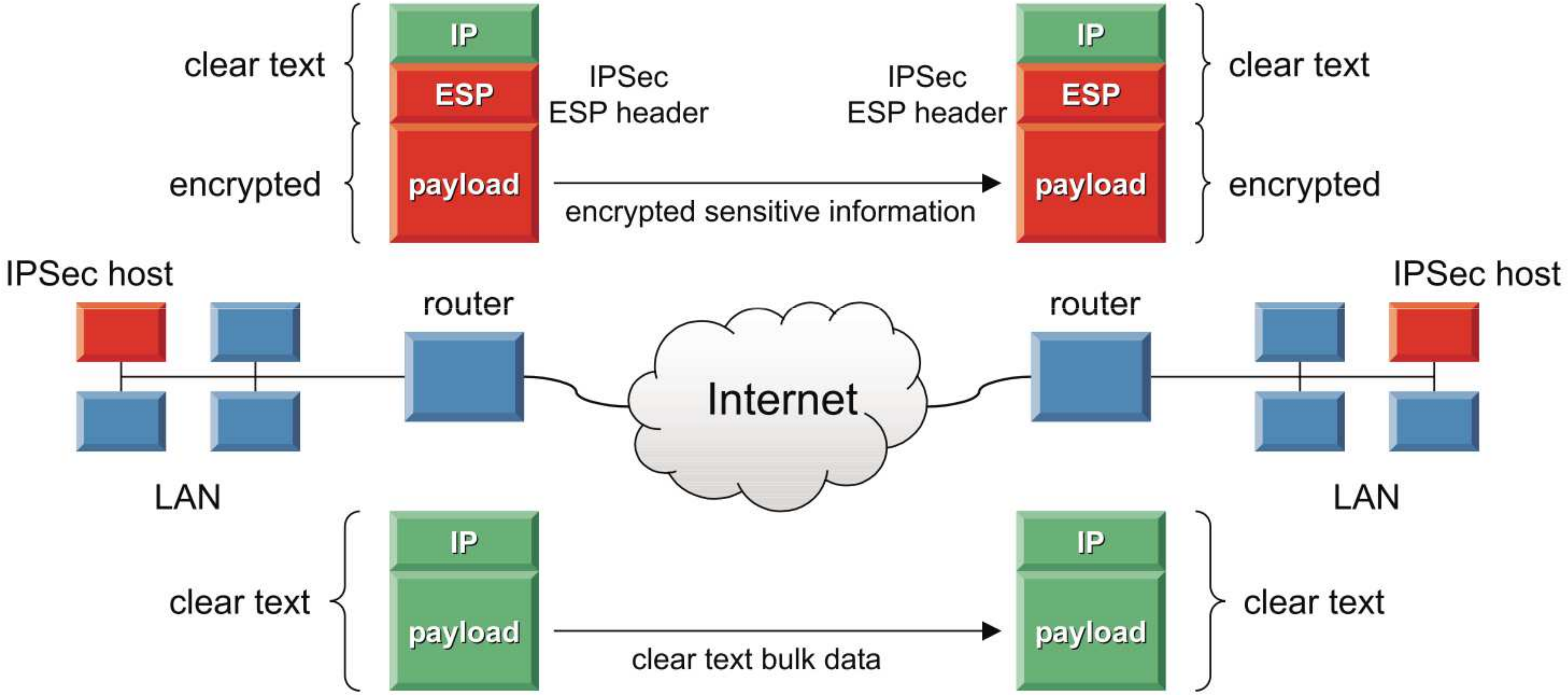
Supports AH and ESP connections
Integrated uCrypt cryptographic library includes DHM, AES, 3DES, RC4, SHA1, MD5
TCP/IP StacK NetIF interface integrates with RTOS, Kernel, User Mode TCP/IP stacks

IKE - an application which generates keys and distributes them securely

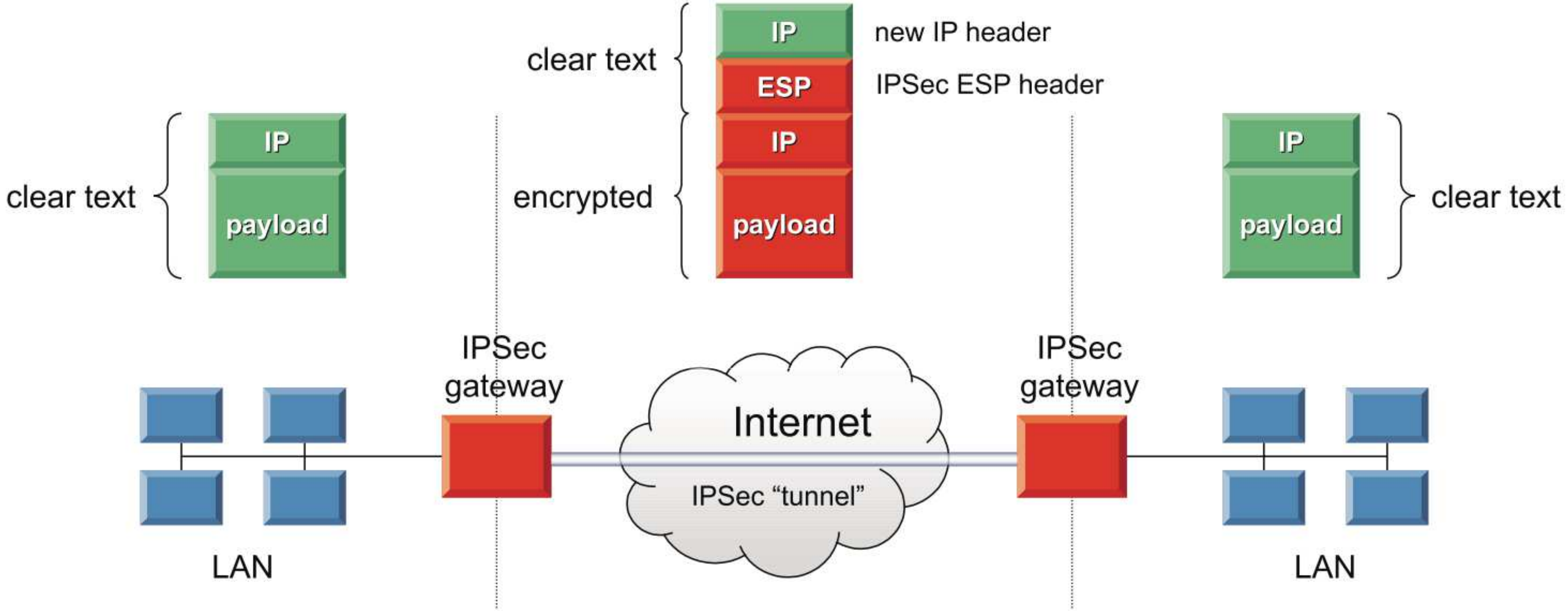
- Security Associations are stored in SA database (SADB), used by IPsec
- Security Policy Database (SPD)
  - governs what security to apply to incoming and outgoing packets
- SAs can be setup in advance
  - no negotiation overhead when applications need secure communication



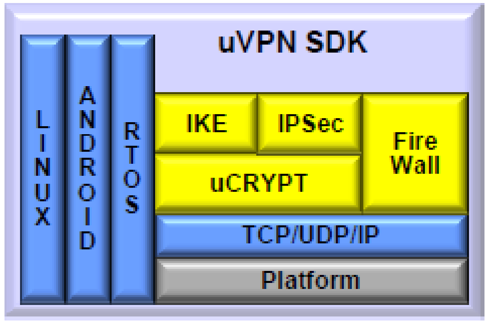
IPSEC / IKE


clear text
IP
ESP
IPSec
ESP header
IPSec
ESP header
IP
ESP
clear text
encrypted
payload
encrypted sensitive information
payload
encrypted
IPSec host
router
Internet
router
IPSec host
LAN
LAN
clear text
IP
payload
clear text bulk data
IP
payload
clear text

VPN



clear text
IP
payload
clear text
IP
ESP
new IP header
IPSec ESP header
encrypted
IP
payload
IP
payload
clear text
IPSec
gateway
Internet
IPSec "tunnel"
IPSec
gateway
LAN
LAN



uVPN SDK
LINUX
ANDROID
RTOS
IKE
IPSec
Fire Wall
uCRYPT
TCP/UDP/IP
Platform

Case Study - Malware Install

- Payment system hacks in large scale retail systems including Target, Home Depot, and others requires new levels of control for software updates
- System is first compromised by hacking into back office systems
- Once hackers get command line, then malware installs from IT systems are downloaded to terminals through software update process
- Terminals fail to authenticate software update
- Malware becomes resident in terminal and works with compromised back office system to steal payment card track information and PINs

SUPERVALU

THE HOME DEPOT

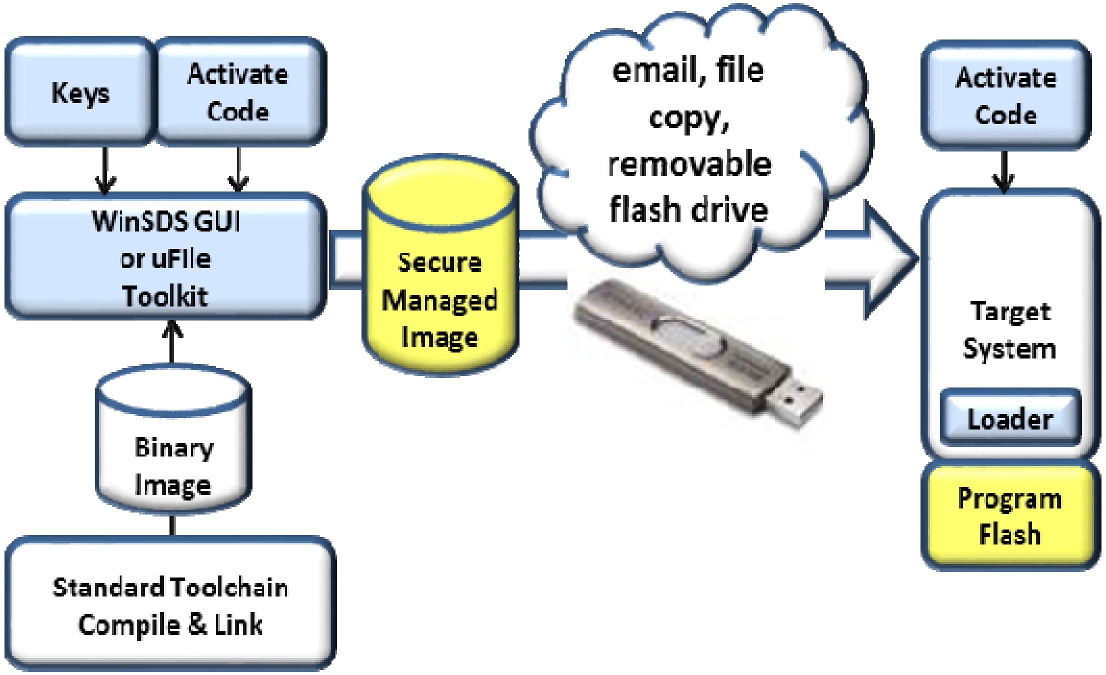
TARGET

Michaels
THE ARTS AND CRAFTS STORE

Neiman Marcus

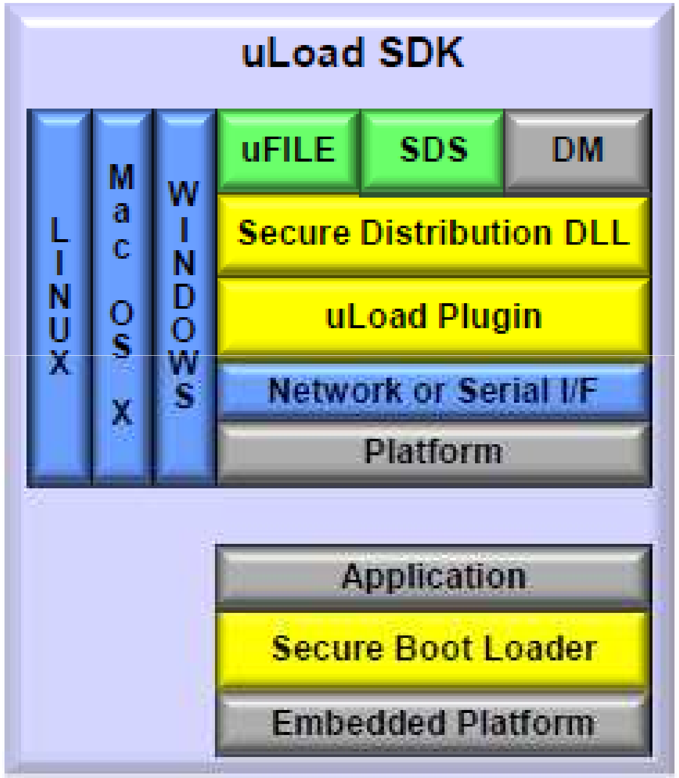
uLoad Install Defender Overview

- ✓LKG and factory image rollback
- ✓Managed registry retains image history
- ✓Power fail recovery
- ✓Manage code images and FPGA bitstream files
- ✓Use standard compilers including IAR, GCC, Keil etc.
- ✓Example porting : NXP LCP1857 (Cortex-M3)


Keys
Activate Code
WinSDS GUI or uFIle Toolkit
Binary Image
Standard Toolchain Compile & Link
Secure Managed Image
email, file copy, removable flash drive
Activate Code
Target System
Loader
Program Flash

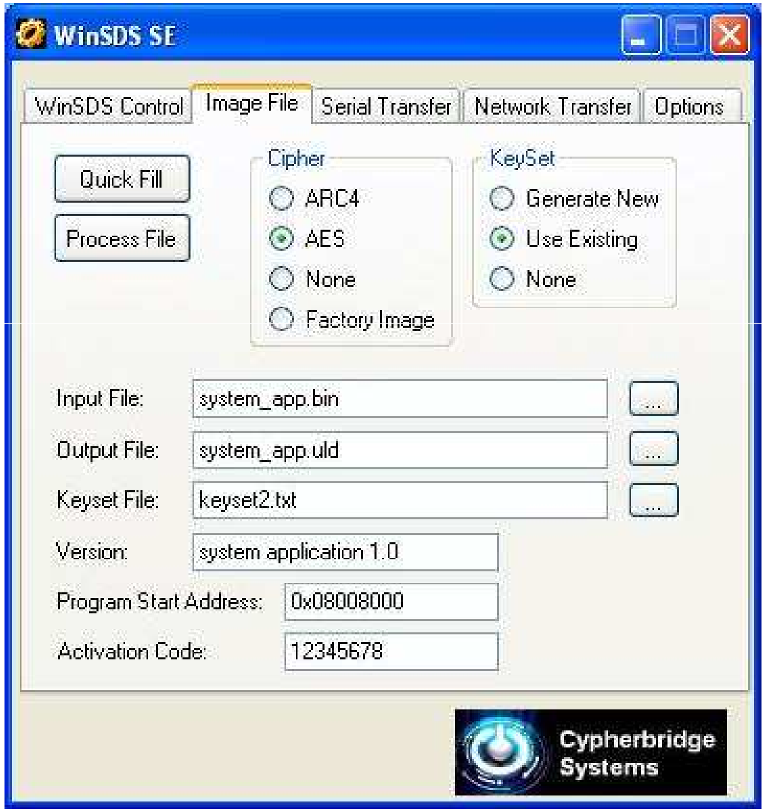
uLoad Install Defender Overview

- ✓ Resident loader in embedded terminal
- ✓ Authenticate safe origin and integrity of software updates
- ✓ Software is installed only if genuine and authorized
- ✓ Multi-level encryption and hashing achieves robust solution
- ✓ Encrypted files on USB or MicroSD flash drives are un-hackable if lost or stolen



Prepare Software Update File using WinSDS GUI or uFile command line Toolkit:

- WinSDS GUI imports compiled and linked binary image from standard toolchain
  E.g. IAR, GCC etc, etc.
- User enters activation code
- Encrypts image and adds managed file header
- Managed file is safe and ready to install !



Cipher
○ ARC4
● AES
○ None
○ Factory Image

KeySet
○ Generate New
● Use Existing
○ None

Input File: system_app.bin

Output File: system_app.uld

Keyset File: keyset2.txt

Version: system application 1.0

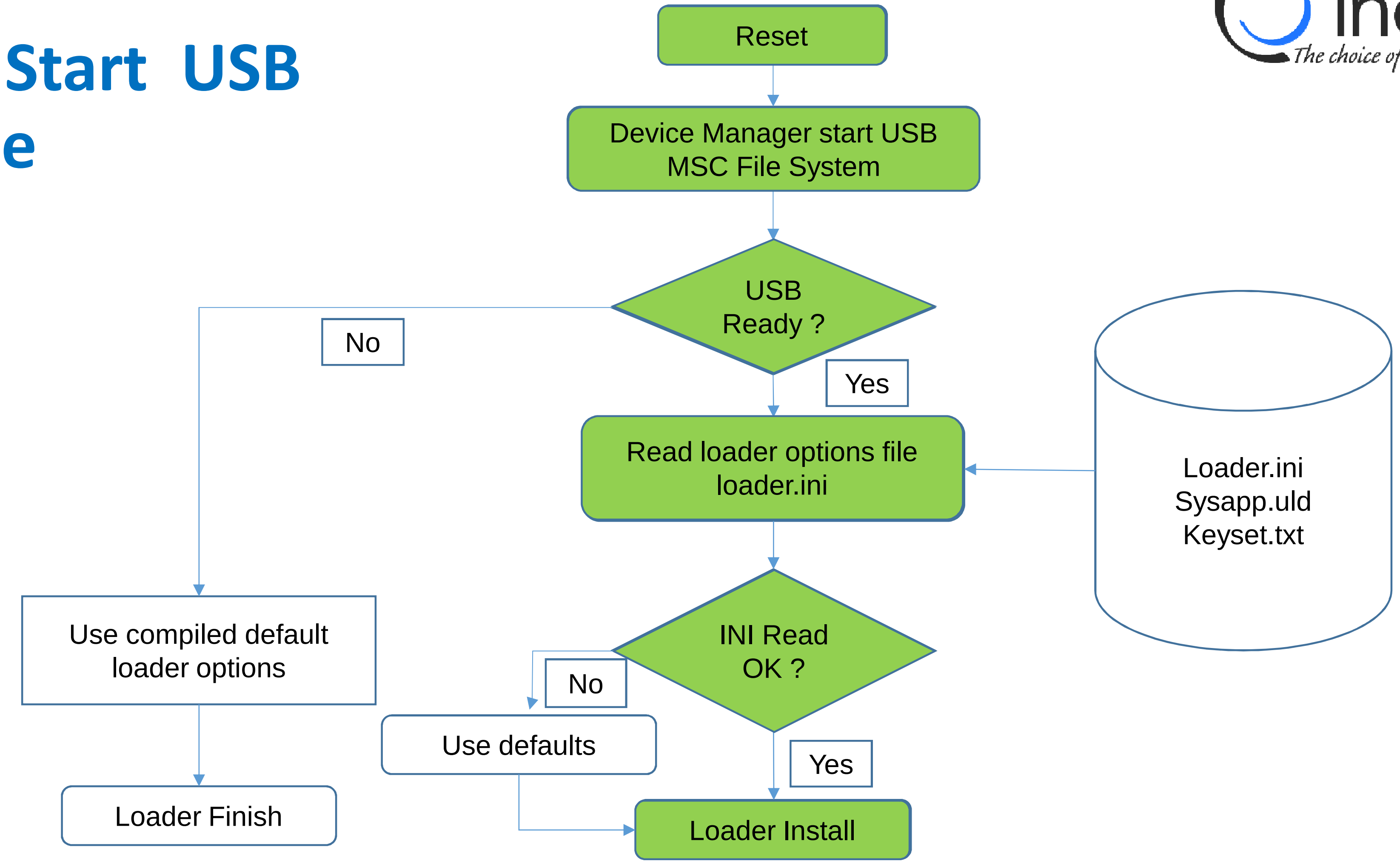
Program Start Address: 0x08008000

Activation Code: 12345678

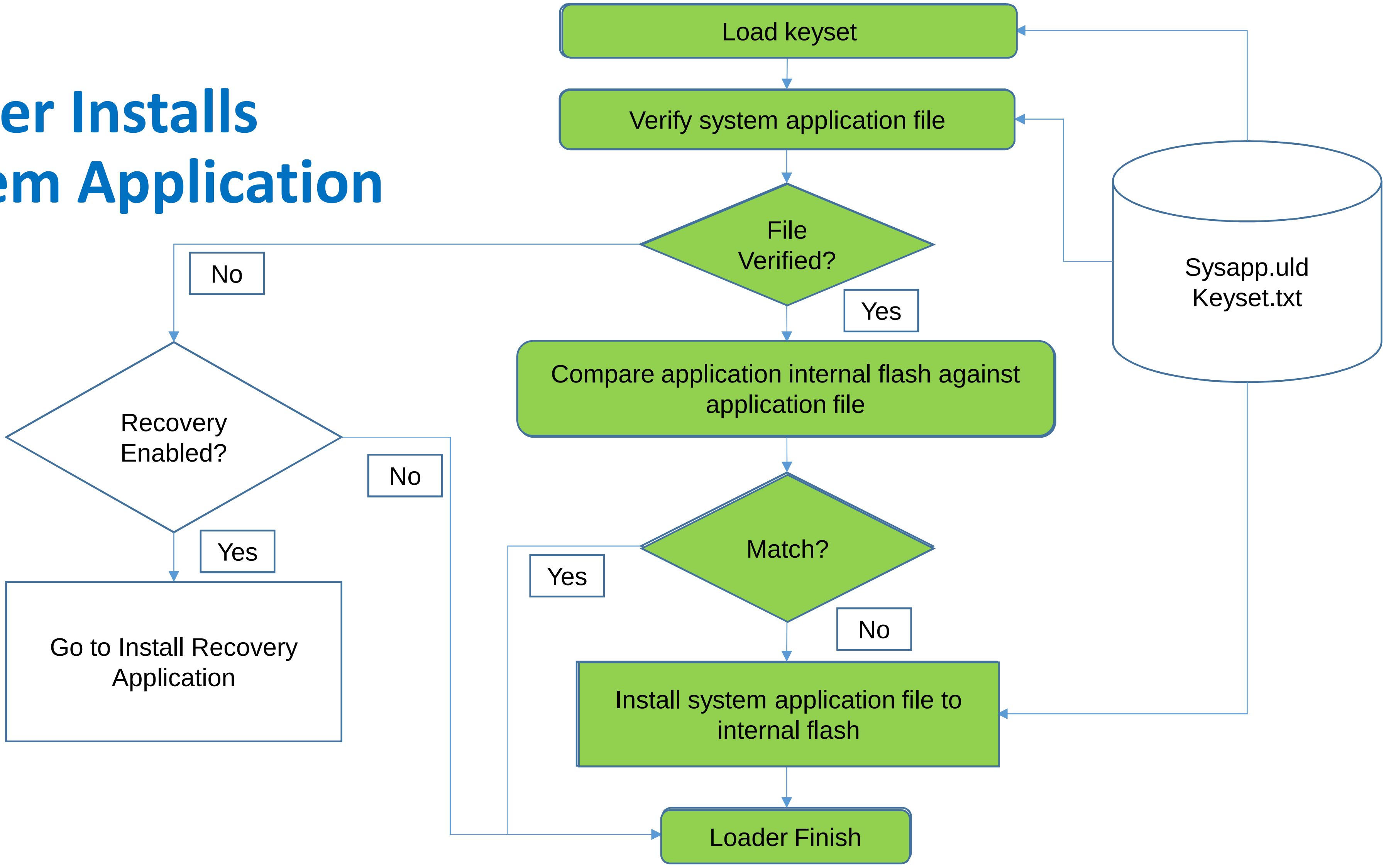
uLoad Install Defender Step-by-Step

- Loader starts at reset, armed with pushbutton hold-down, reads loader.ini options and file names from USB or MicroSD flash drive
- Loader verifies external system application file integrity using managed image header and keyset
- Loader verifies internal application against managed image files. Must exact match SHA1 hash. If verify fails, loader reads application file from USB and writes to MCU internal flash.
- Loader jumps to system application start address
- Loader failsafe jumps to system application if any load steps fail

Loader Start USB Example


Reset
Device Manager start USB MSC File System
USB Ready ?
No
Yes
Read loader options file loader.ini
Loader.ini
Sysapp.uld
Keyset.txt
INI Read OK ?
No
Yes
Use compiled default loader options
Use defaults
Loader Finish
Loader Install

Loader Installs System Application



Load keyset

Verify system application file

Sysapp.uld
Keyset.txt

File Verified?

No

Yes

Recovery Enabled?

No

Yes

Go to Install Recovery Application

Compare application internal flash against application file

Match?

Yes

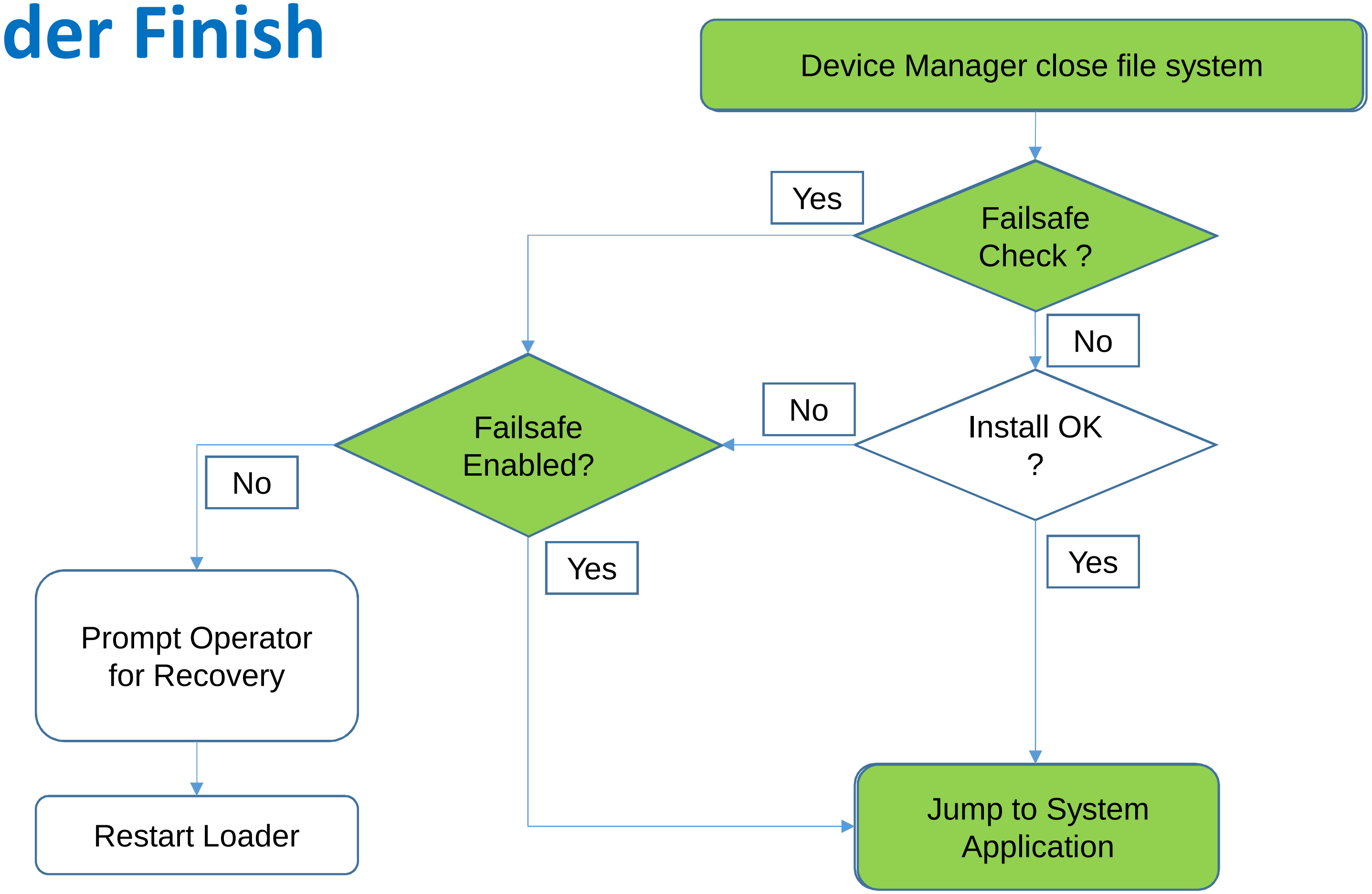
No

Install system application file to internal flash

Loader Finish

Cypherbridge Systems

Loader Finish

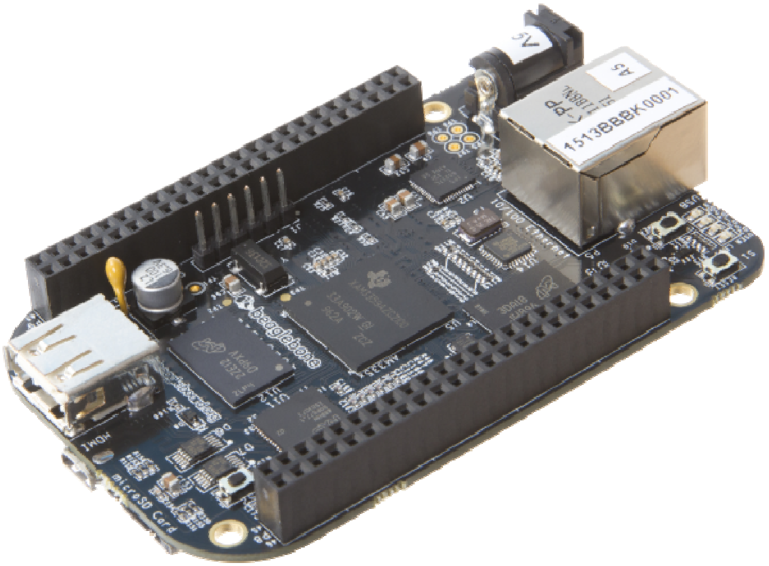


Device Manager close file system
Yes
Failsafe Check ?
No
No
Install OK ?
Failsafe Enabled?
No
Yes
Yes
Prompt Operator for Recovery
Restart Loader
Jump to System Application

Nice..

But how do I add this to my embedded system ?

- Can’t I simply download this all from the internet ?
- Embedded systems can be very resource constrained
  - Memory footprint
  - Performance
  - Power Budget
- Integration in my embedded application
  - Drivers & RTOS integration ?
  - Integration with IP-stack
  - Integration with application code
- Is all this not very complex ?
- I am in a hurry to get to market!!



- **Integration & porting examples :**

- Texas Instruments MSP430, Stellaris Cortex M3, Sitara CA8 and ARM9. DSP BIOS/NDK platforms including DM642
- NXP3250 ARM9, LPC175x, LPC1768, LPC1788, LPC18x57
- ST Microelectronics STM32F2xx and STM32F4xx
- Freescale Kinetis K60
- Renesas M16C, RX62N
- Atmel AT91SAM
- ADI Blackfin
- Evaluation boards from Freescale, STMicro Eval and Discovery, TI, NXP, Phytec, Keil, Atmel, Embedded Artists, Critical Link, and more!

Compiler, IDE and middleware agnostic

IAR SYSTEMS

SCIOPTA

HCC embedded

WIND RIVER

DIAB DATA
Defining Compiler Performance
An Integrated Systems Company

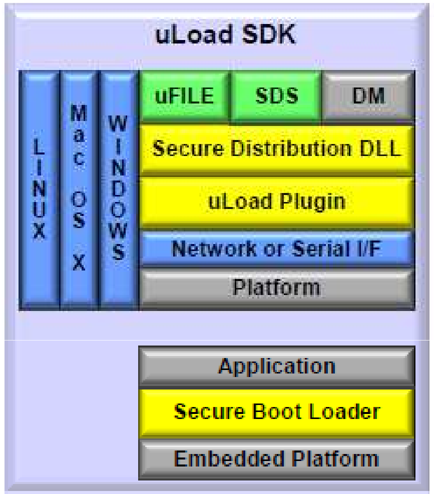
GCC

KEIL™
Tools by ARM

SEGGER

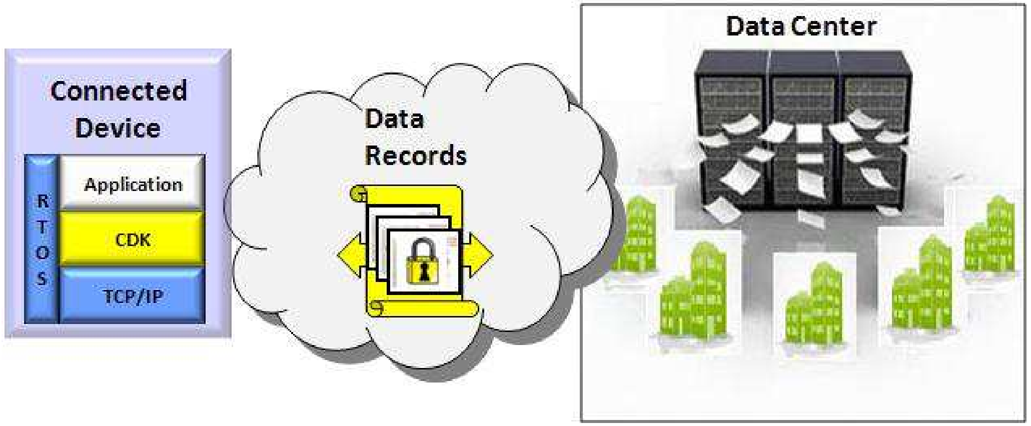
Cypherbridge Systems

Integration & time-to-market :
- SDK's and Toolkits



✓uLoad – Safe software loader and installer blocks malware & unlicensed updates

✓CDK – Cloud Toolkit integrated end-to-end solution to enable devices to connect securely to the cloud, to synchronize and replicate files



indes
The choice of professionals

Integration & time-to-market :
- Vertical Solution packages and customer examples

- ✓ Electric Vehicle Charging Solution
  - ✓ uSSL SDK, Control firmware & TCP-stack on Renesas M16C65
- ✓ Smart Meter Security
  - ✓ uSSL SDK, Embedded RTOS & TCP-stack on STM32F207

- ✓ Scada Secure Telemetry
  - ✓ uSSH SDK, Embedded RTOS and TCP on STM32F407

- ✓ AK200 Point-Of-Sale Terminal Platform
  - ✓ provides a low-power, low-footprint approach to wirelessly secure payment transactions in embedded devices.
  - ✓ AK200 includes a nationwide cellular data plan in partnership with Wyless Group, an M2M managed service provider.

INDES-IDS BV - QuickStart service

- On-site assistance in setting up Tools, RTOS and middleware
- We can do the integration with your platform and application for you
- Local expert support
  - You give us (prototype) hardware so we can locally reproduce problems and support you
- Fixed price integration services

indes
The choice of professionals

For more information contact:

sales@indes.com

Tel : 0345 – 545.535

www.indes.com/embedded

Cypherbridge Systems