EB Security services, competences and references

Marko Nivalainen
16.8.2013

Elektrobit

Background - What is security ?

- Security is **not** a single thing that you can turn on or off. Instead, it is step by step process of controlling what you want to allow and disallow
- Security requires building a long chain of steps fulfilling security requirements starting from the hardware, ending to user applications
- And as with other chains, it is only as good as its weakest link
- EB offers services for developing of secure platforms, devices and secure applications. Next slides describes available services, key competences and selected references

EB has been analyzing, designing, integrating, testing and manufacturing various embedded wireless devices for over 25 Years for both the mass – and special markets such as public safety, defense and security.

EB Wireless

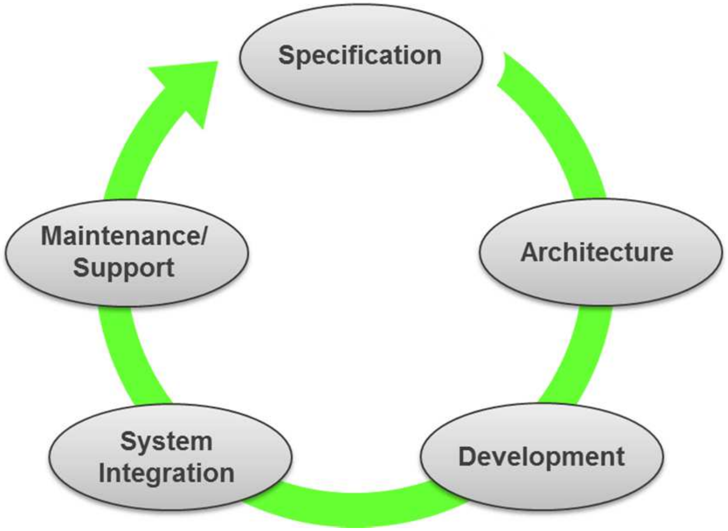
Security services

- EB Offers security services in following areas
  - Security requirement management
  - Secure system design, architecture design
  - Secure Hardware design
  - Security SW implementation in different platforms including but not limited to mobile device, base station and small wireless devices platforms
  - Security planning and implementation for device manufacturing and maintenance

  - In next slides more details from these services

Security services - Requirement management

- Typical project in EB starts with specification phase where requirement management is essential part of project. If customer has special requirements for security, requirements are defined together with customer
- FIPS and Common Criteria requirements is used as baseline ..\..\..\Projects\StarComm\Security\Standards
- Also operator security requirements for mobile devices is used as guideline
- EB offers security requirement management support for different platforms, for example TI OMAP, Renesans, Intel.

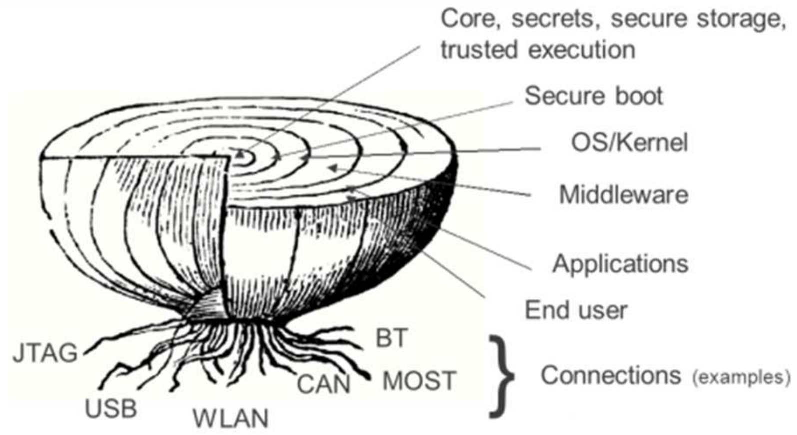


Security services - System and architecture design

- System and architecture design for security starts in EB by threat analysis
  - In threat analysis it is evaluated possible security risks related to system under development
    - Threats can be divided to following (not full list, some examples):
      - Tampering, modifying of platform
      - Unauthorized use of platform, debugging
      - Jamming of platform or some specific feature
      - Unauthorized SW in platform, re-flashing
      - Unauthorized changes in platform configuration
      - Platform copying
      - Unauthorized communication
    - Typical security threats can be found from attached OMTP document

      Adobe Acrobat Document
  - As a result, additional requirements for system security is created

Security services - Security architecture



- Each layer and connection in architecture picture presents item which is under possible security threat.
- Security can be reached by protecting layer by layer and all connections from threats, security is as weak as weakest layer and connection in security chain
- Security can be reached by chain of control – Hardware ->Boot loaders -> Operating system -> Middleware - > Applications

The chain of security starts at hardware:

– The hardware needs to be tamper proof to disallow bypassing its security features

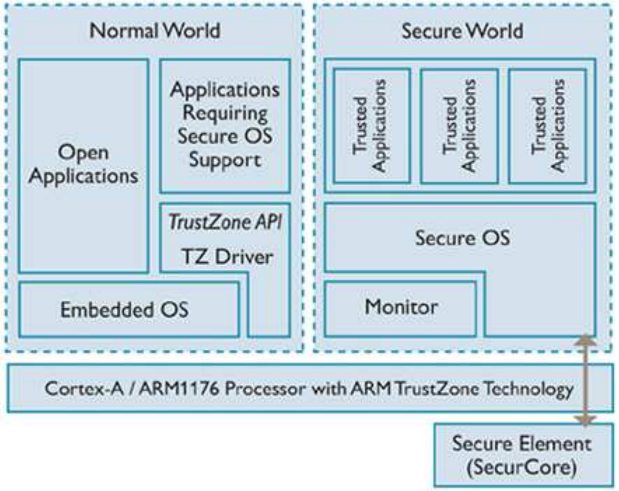
– The hardware needs to have enough security features to allow controlling what needs to be controlled

– The hardware should provide secure storage (for keys and other sensitive data) and other features required by later steps

– The hardware also needs to authenticate the first part of the software run after power on, the boot loader

Security services - Secure architecture example OMAP

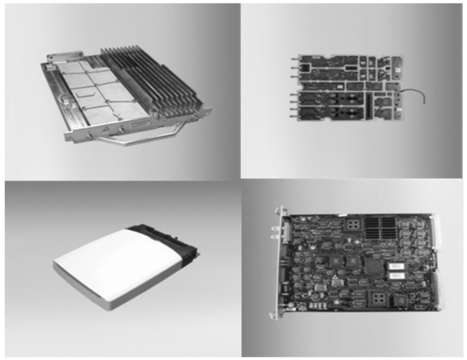
- Most mobile chipsets are ARM based. The general security solution for modern ARM processors is called ARM TrustZone. That includes the low level HW & FW needed for platform security such as secure boot, secure storage etc.
- OMAP 4 is ARM based SoC and therefore embeds ARM TrustZone. Security framework is called M-Shield and it complies with Trusted Foundations security specifications. M-Shield is applied on top of ARM TrustZone.
- M-Shield provides complete platform security solution with Trusted Execution Environment (secure storage & execution), cryptographic accelerators, secure boot, possibility to secure debug interfaces etc.
- EB has access to full M-Shield development kit and the necessary documentation. Documentation is very through and solution seems mature & stable.



Security services - Secure hardware design

- Typically in R&D project/program there is two different HW. R&D boards and secure boards.
- In R&D HW all interfaces are open and layout and other design is none in normal way. R&D HW is typically used in SW development and other purposes.
- In Secure HW interfaces are closed or protected to full fill security requirements. Critical lines is layout are protected or hided, debug interfaces are removed.
- In high level security HW there are also mechanical and other protections. Basically in tampering HW will destroy it self.
- Secure HW requirements must be taken account also in production

EB has lot of experience of planning secure HW for different platforms. See references for more details

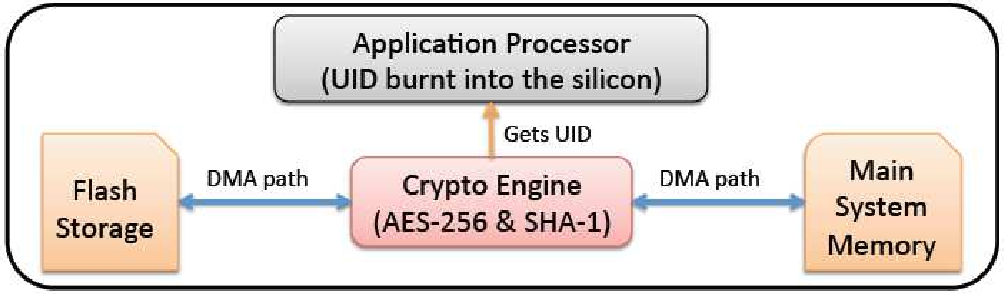


Security services - Security SW

- EB offers secure software design in many areas of secure SW
- Following slides describes implementations done for example in mobile devices. EB has experience of implementing these security feature for example to android devices, Windows phone platform and also for base station platform
- EB has also done several military devices which implements features describe in following slides

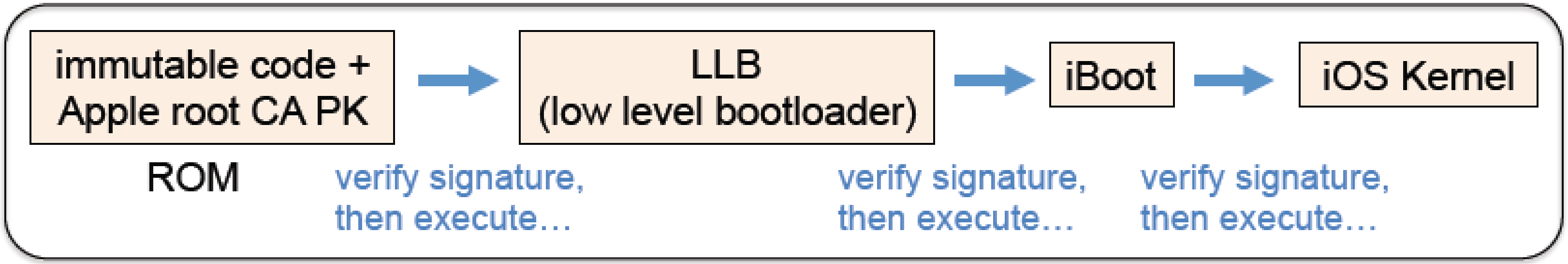
Security services - Security SW, HW interfaces

- In HW platform we have many different processors and each of them must be protected by SW
  - Protection of each processor is based on secure boot and chain of trust
  - Protection of system is based on authenticating processors in system
  - Each processor can authenticate each other, if authentication fails system is halted to prevent unauthorized use.
- Each processor has HW interfaces which must be security protected by SW
  - Different mechanisms are used to protect each interface
    - Memories – crypting, hashing
    - WLAN, BT, Modem protocols – authentication, Firewall/Virus protection SW security
    - USB(s), UART(s) – Authentication, Firewall/Virus protection, application security
    - JTAG – Disabled in commercial product, processors secure fused



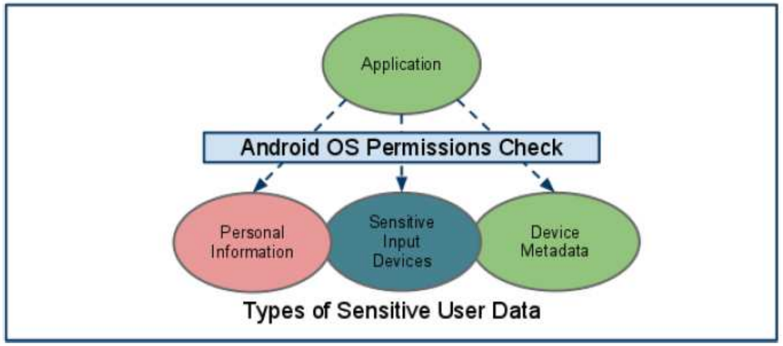
Security services - Security SW, bootloaders

- Boot loaders are the first part of software that is run on device after power-on
- Boot loader initializes the hardware to known state and then loads the rest of operating system
- To prevent unauthorized software to be run on the device, the boot loader authenticates the OS image it loads
- If the boot loader itself is in several parts then each part needs to authenticate the next one before executing it
  - Modifying the first part of the boot loader after the device is shipped might be hard or even impossible (it is authenticated by hardware, and it might even be stored in read-only memory)
- Authentication requires hardware to provide storage for keys or checksums of authorized keys



Security services - Security SW, OS and other SW

- Operating system is the authorized software running on the device
- OS has full control of the hardware, so it needs to control what applications are allowed to run and do
- If implemented correctly, even the OS does not have direct access to keys or other data in secure storage provided by hardware, but it still needs to control what software can use those
- The OS can command the communication channels (modem, bt, wlan, ..) and needs to control what applications may do with those
- Even OS allows application to run, it may contain components which may illegally try access HW or communication interfaces
- Access to HW and communication interfaces is protected by using middleware software components which checks if access is allowed

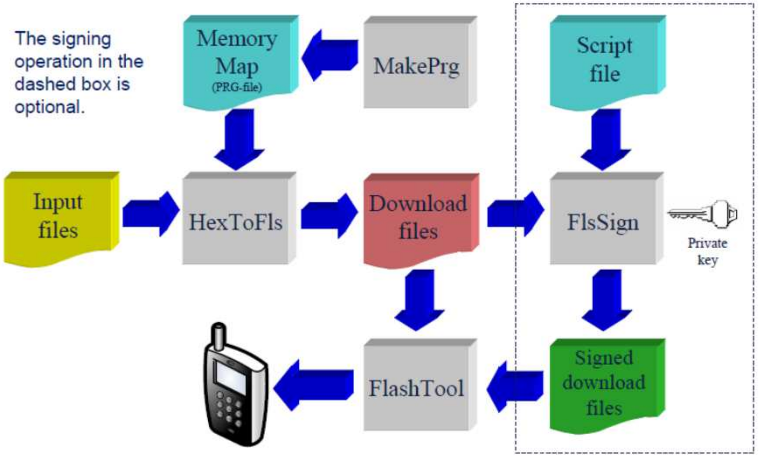


Security services - Secure device manufacturing

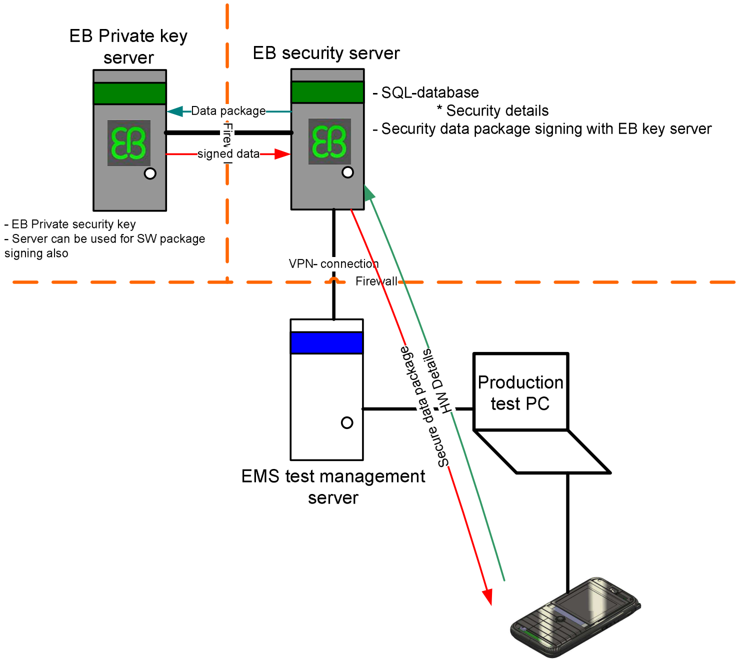
- Requirements for secure device production covers items from all areas in system
- In EB there is existing environment where secure device production is possible almost in any factory
- Usually secure device production needs device specific certificates, keys, signatures, etc security related data
- Security related data is stored to device in production
- Next slides describes system created by EB, example system is created for mobile phone. Same system can be used for wireless device or base station mass production

Security services – Secure device manufacturing example, mobile phone

- Secure build environment
  - Needed to make secure data package which is written to device in production
  - Used to create secure SW image, certificates, keys, etc
  - Device uses secure boot, IMEI protection, SIM locks, etc features to protect phone
  - Device protected against unauthorized copying



Security services – Secure device manufacturing example, mobile phone



EB Private key server

- Only for secure data package and modem SW signing (Signing module)

EB security server

- Product identification
- Server sends information to EB Private key server for secure data signing (Signing module)

EMS Test Management System

- Requesting secure data package for this specific phone with security details
- Production testing PC sees only IP-address through EMS Test Management System
- Saves all test data from production line

Production test PC

-Handles all sequential material and drivers for using SW and HW

- All communication methods and components are in this PC. Couple of new testing components needed

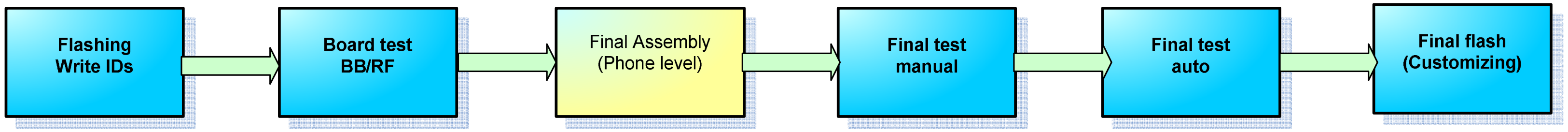
Target Mobile

-Identified with HW details

- This ID and generated serial number will be sent to EB's secure server

-Secure data package will be generated in EB's secure server and delivered to mobile

-Security setup to Mobile will be made in last Final Flash Station



Security services – Secure device manufacturing example, mobile phone

Security management in production line

EMS: Production Management System

HW details will be read from Phone -> Phone serial number is linked to HW details

- Phone serial number and HW details will be delivered to EB's security server

- EB's security server generates signed security data package to this specific phone

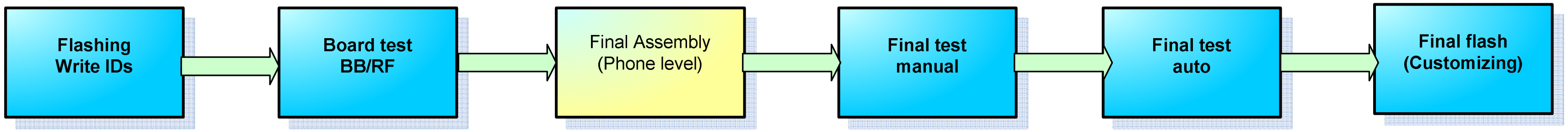
- In final station this current signed security data package will be written to this specific phone

*** Phone identification have to be made using Phone serial number in production**

EB’s security server

- EB's security server includes SQL-database containing phone specific HW details, lock codes, etc security related information (For production and AMS purposes)

- **AMS will need same security server connection as Production has.**
- **All communication between mobile and Security server is crypted!**

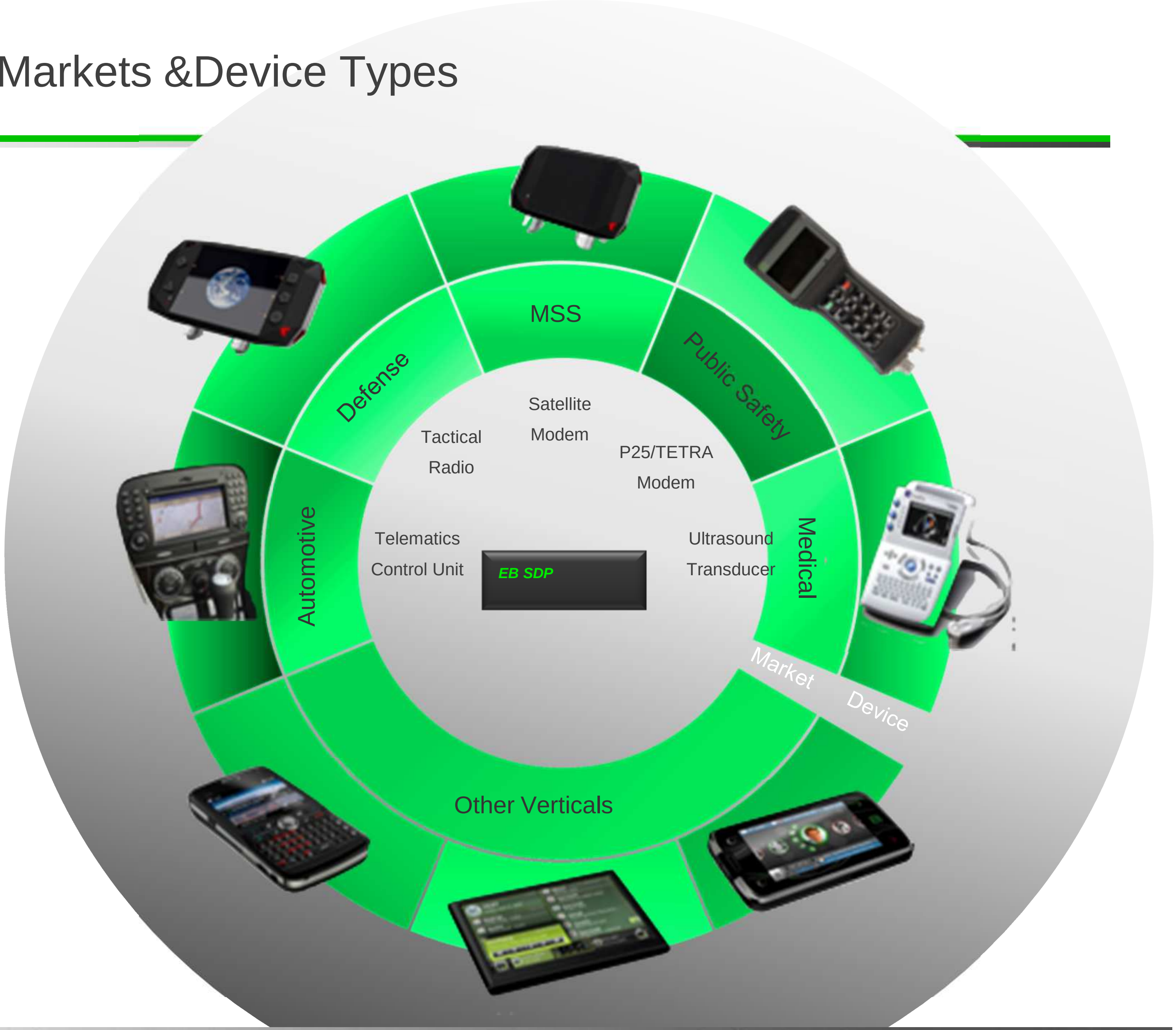


EB Wireless References

EB Specialized Device Platform (SDP)

- EB has developed a specialized device platform (SDP) targeted for a variety of vertical market customers within the Specialized Terminals business area of EB’s Wireless Solutions business unit
- The SDP is a technology platform that comprises the primary components in a smartphone-type mobile device system – high performance/low power processor, advanced security architecture, touch-screen display, cellular radio, Bluetooth radio, Wi-Fi radio, GPS, audio, various sensors, battery/power management, and typical system interfaces
- The platform is highly secure, scalable and configurable, and is designed to support longer product life cycles to better serve the various target vertical markets, including ruggedized, industrial, government or defense applications

EB SDP Target Markets &Device Types



Reference I
EB SDP based product: Raptor ID

- The RaptorOne™ handset and RaptorPad™ tablet are the result of pairing an SDP configuration with Raptor ID's application specific sub-system features (biometric scanners)
- EB is responsible for design and supply of the products
- The EB SDP enabled Raptor ID to leverage the technologies and economies of scale of the cellular market with feasible up-front costs to enable their product offerings
- Both products are based on an SDP configuration using the OMAP4460 and Android 4.0 (Ice Cream Sandwich)
- EB is about to deliver another SDP based product to a well known aviation company. Gaining highly secure architecture is priority 1 for the customer.

"The technology EB has packaged into the Specialized Device Platform is a disrupter for the specialized government markets because it is a customizable, cost-efficient platform that enables us to incorporate our advanced secure and classified biometric technologies. EB's platform is cost-effective and allows fast turnaround, which helps government agencies stay current with their handheld devices. Rather than developing small batches of high cost, highly specialized product, EB's platform allows us to integrate low cost modular attachments to meet the needs of specific agencies, while simultaneously producing high volumes of core products at substantially lower cost per unit.“

Charles Strasburger, Chairman and CEO of Raptor ID

For more information on the Raptor ID products, please visit www.raptor-id.com

Reference II
EB Rugged VoIP terminal for Military Use

- Linux based, fully rugged and environmentally shielded IP phone product
- Provides standard SIP based VoIP peer2peer calls with prioritized group call modes
- Dynamic phonebook contains all the current roles in the network in real time.
- Remote upgrade capabilities: Manually, through Web-based management and as unattended automatic software upgrade from remote server (OTA update)
- Networking and control support: IPv4, TCP, UDP, ICMP, ARP, DiffServ/ToS, SNMPv1/2, SNMPv3, MIB II (RFC 1213, RFC 2011, RFC 2012, RFC 2013)
- *Security & Encryption*: DES/3DES/AES standards and Secure RTP (RFC 3711)
- EMI MIL-STD-461E (RE102, RE103) Navy Mobile & Army, Navy Fixed & Air Force

Reference III
EB Wireless Access Point for a car OEM

- EB designed, manufactured and maintained, highly secured and reliable wireless communication link between a car and wireless tools used in the workshop and/or production area and all connected to main servers of the car OEM via wireless Access Point (AP).
- WLAN AP based on 802.11n customized to be compatible with customer specific secure technology for secure wireless connection between all tools of the system and towards main servers of the system.
- Continuous improvement of the system together with customers
- EB provides 36 months warranty for the product.
- Faulty products replaced globally within 24, 48 or 72 hours (depending the area).
- First line support available 24/7/365.

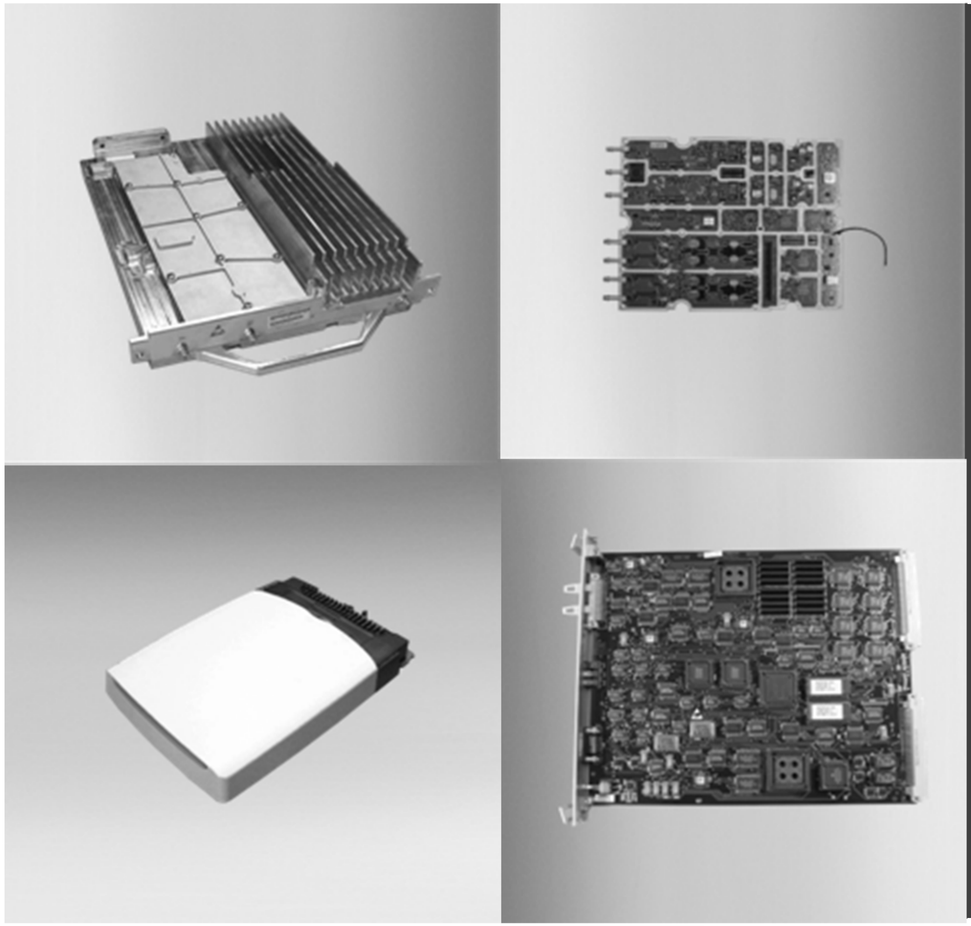
Reference IV: TETRA Vehicular Terminal

- TETRA provides authentication of terminals towards infrastructure and vice versa. For protection against eavesdropping; air interface encryption and end-to-end encryption are supported.
- EB responsibilities
  - ✓ Complete product concept creation and design with accessories
  - ✓ Verification and Validation
  - ✓ Official certifications and type approvals
  - ✓ NPI
- End customers: Police force and fire brigade

Reference V
EB Satellite-Terrestrial Smartphone

- EB designed, manufactured and maintained world’s first satellite-terrestrial handset with form factor addressing mass-market
- The smartphone is based on the highly flexible and secure EB platform and can be easily customized for specific target markets.
- Communication interfaces supported: GSM, 3G, S-band satellite, Wi-Fi, Bluetooth, USB and GPS.
- Provides solid network level encryption of sensitive user data, as well as complete topology hiding for both TerreStar and customer services infrastructure. It integrates with other device, application, and user identity-oriented security methods.
- End customers: homeland security and defense, fire brigade, police and disaster recovery groups.

Reference VI: Infrastructure experience



- EB has delivered several and complete GSM and WCDMA basestation products under Original Design and Engineering (ODE) business models
- EB is currently working to deliver three complete LTE basestation products to customers
- Security related items have been handled by EB and by EB's partner

Get in touch!

Contact us:
www.elektrobit.com

Marko.Nivalainen@elektrobit.com