dresden elektronik

*Erfolg lässt sich steuern*

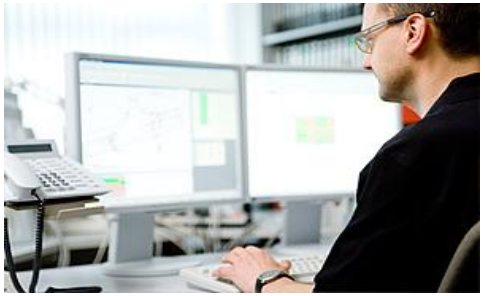
# Security Framework for IP based Wireless Sensor Networks

Mike Ludwig
dresden elektronik ingenieurtechnik gmbh
www.dresden-elektronik.de

# Dresden elektronik

dresden elektronik ingenieurtechnik GmbH

- founded: October 1990
- employees: approx. 90
- profile: hardware/software development
  manufacturing
- location: Dresden, Saxony



Presenter

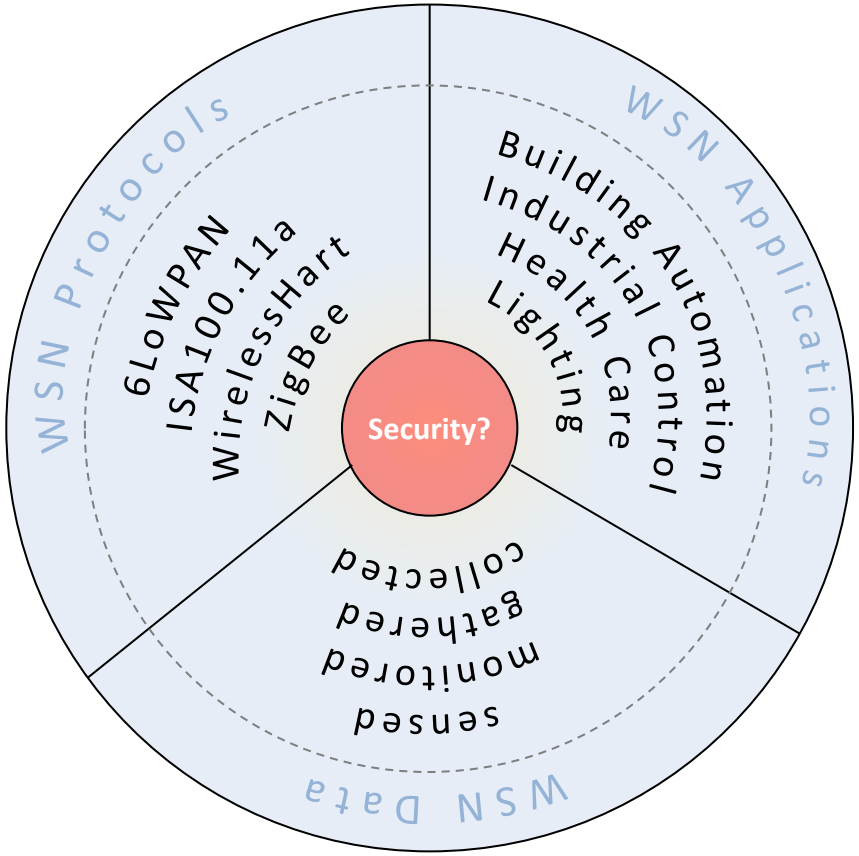
- name: Mike Ludwig
- position: team leader research
- profile: software and hardware design
  for ultra low power devices and
  wireless systems
  more than 7 years of expertise
  in wireless sensor networks

# Content

- Motivation
- Security architecture in wireless sensor networks
- Framework concept
- Packet flow
- Framework modules
- Security algorithms
- Conclusion

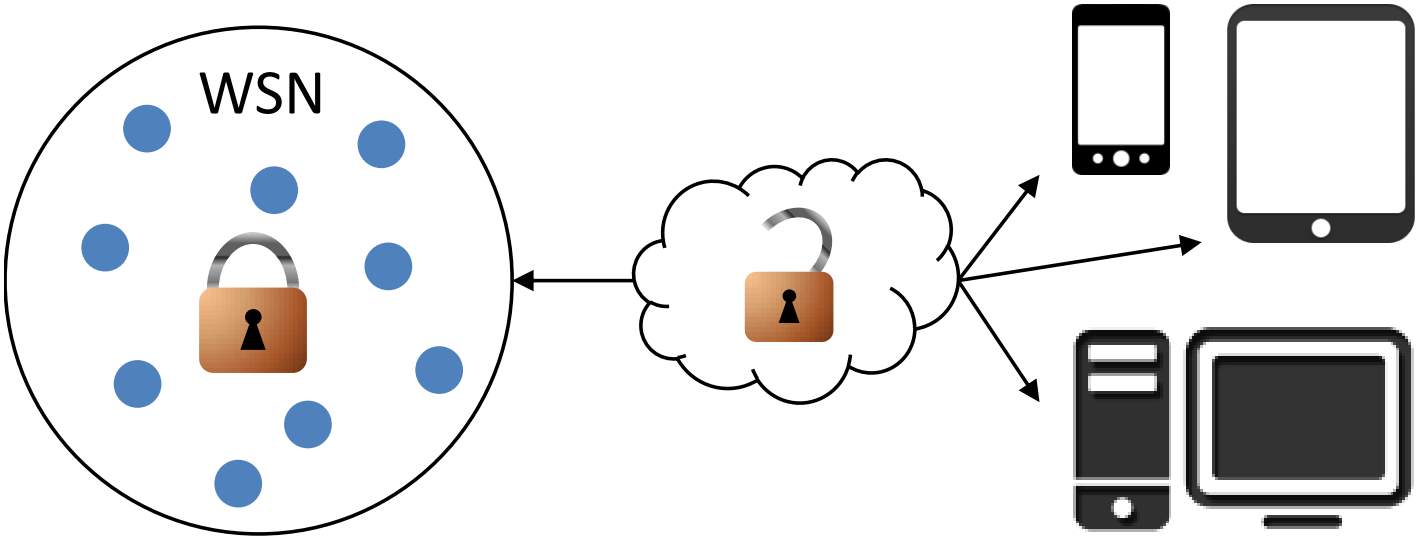
# Wireless Sensor Networks Application Fields

- WSN have different protocols, applications and data
- there is no common way to secure data



# Wireless Sensor Networks and Security

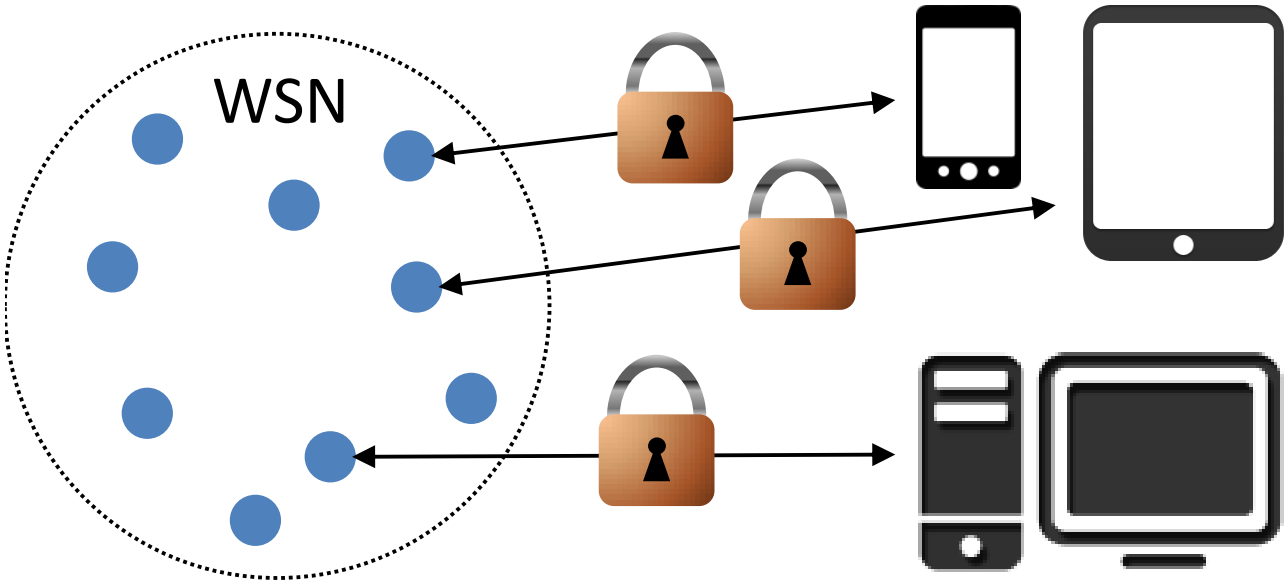
**Common way** is to secure inner WSN communication




- Drawback: Secure communication ends at WSN gateway
  → unsecure data transmission to business application

# Wireless Sensor Networks and Security

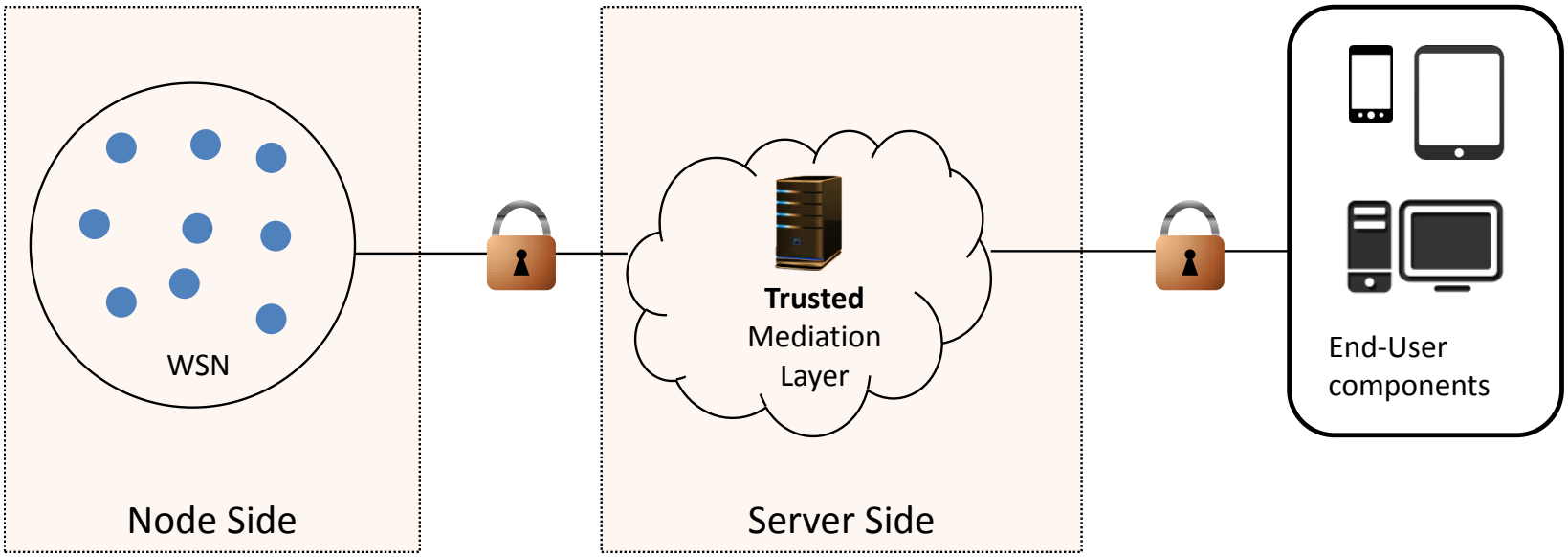
**Preferred Solution** is to use end-to-end security




- Advantage: Secure communication between business application and WSN node.

# Security Framework Concept

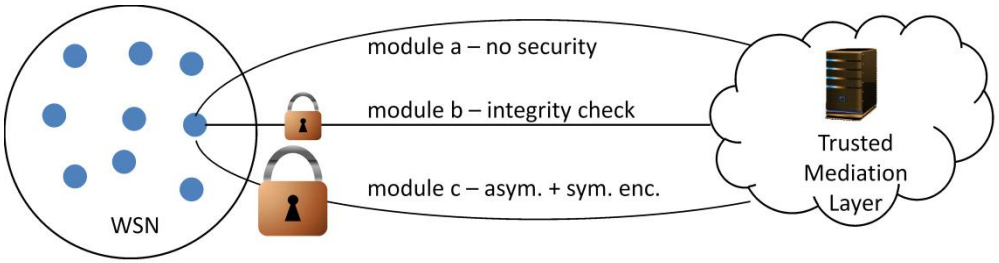
**Our framework** currently provides a hybrid approach:




- Advantage: resources for end-to-end security are required at the mediation layer which allows for many (unlimited) end-user components
- Drawback: not real end-to-end security (mitigated by a trusted mediation layer)

# Security Framework Concept

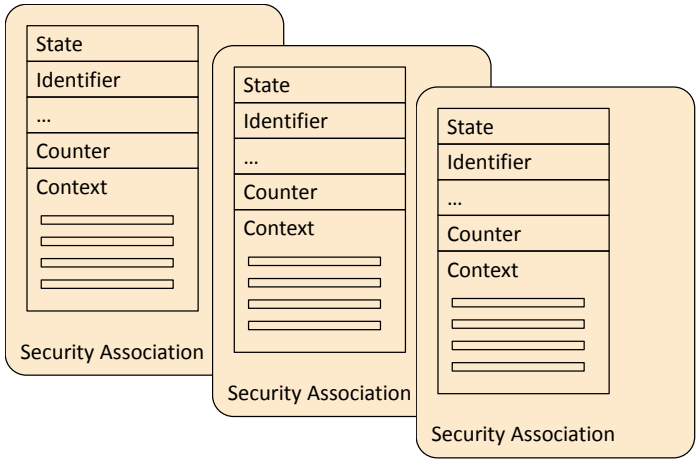
- the framework defines different services (currently 10 different services)
  (parameter transport, data transport, authentication, key management, threat detection, Over-the-Air Update, …)
- each service uses a node and server module (individually configurable)
- each module can have its own security settings
  (e.g. key management asymmetric authentication and symmetric encryption, OTAU uses integrity check only, …)




- security can be selected within a wide range
  - no security
  - integrity check
  - symmetric encryption
  - integrity check and symmetric encryption
  - asymmetric authentication (integrity check)
  - asymmetric authentication (integrity check) and symmetric encryption

# Security Framework Concept

- security is opaque to the application
- the framework stores all security information in Security Associations (SA) (one SA per module)

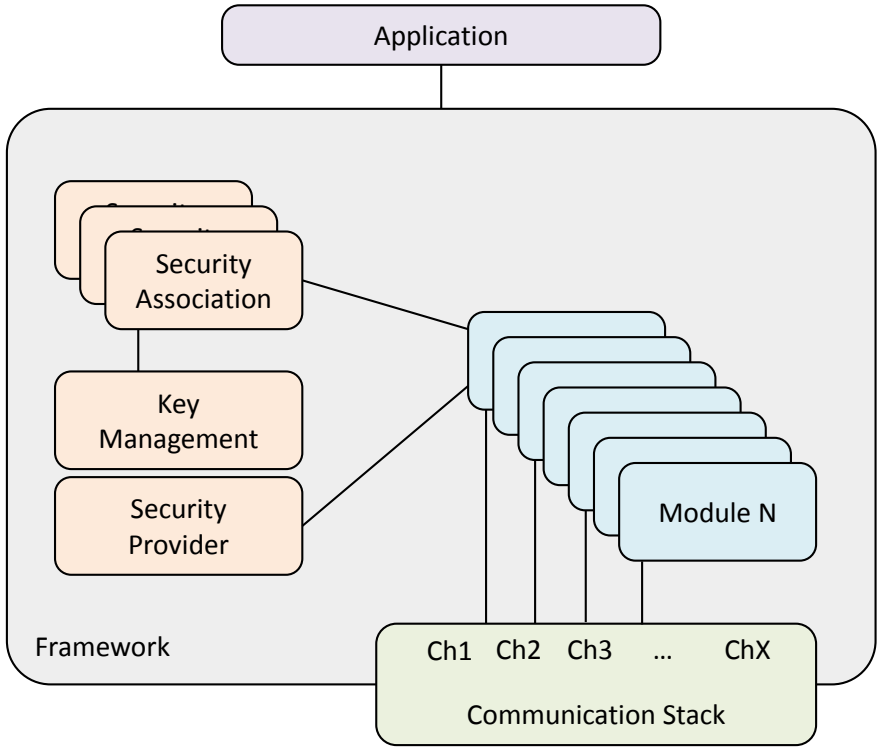



- all SA are established by the key establishment module
- all SA are managed by the key management module
- all SA are interpreted by a security provider (applies and checks the security)
- the application and the framework modules do not need to know about security at all

# Security Framework node-side

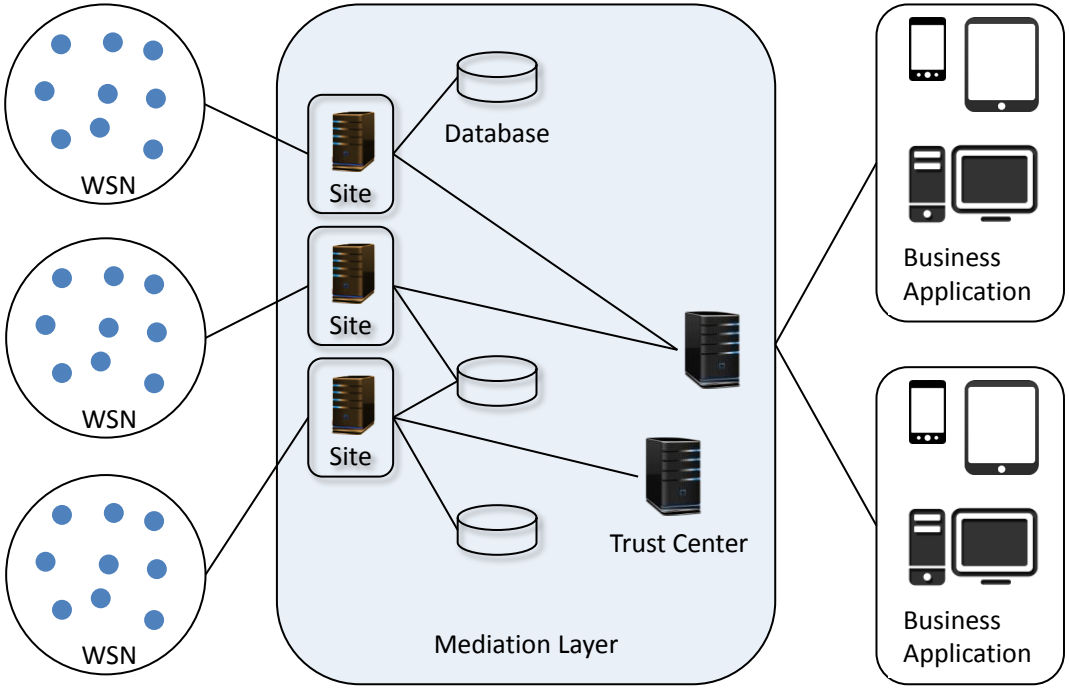
- the framework is mostly communication stack independent
- a module communicates over some ‘communication channel’ with the corresponding module of the mediation layer
- what a ‘communication channel’ is defines the underlying communication stack

- ZigBee: endpoints
- IP: ports
- any other: …



# Security Framework server-side

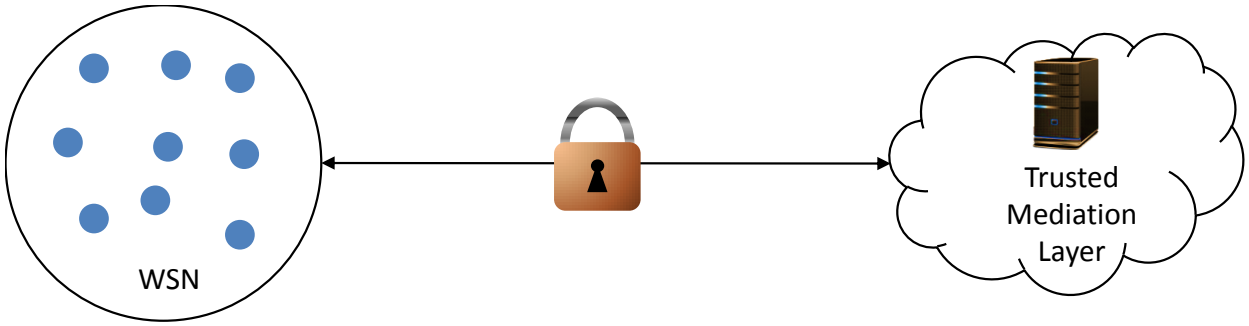
- distributed mediation layer allows connection of WSN from many places
- internal communication is message based (easy transport over different mediums)



# Security Framework – Packet Flow

Example for IP based communication:

- a packet arrives at the UDP layer
- the UDP layer hands it to Network Access Control (NAC)
- NAC gets the SA for the particular source address from Key Management and checks the access policy and validity (using the Security Provider)
- if the check succeeds the packet is passed on (for the module to receive)
- if the check fails Threat Detection is notified and the packet is dropped
- the receiving module gets the SA for the particular source address and module from Key Management and checks the security (using the Security Provider)
- if validation succeeds the data is processed by the module (and may given to the application)
- if validation fails Threat Detection is notified and the packet is dropped

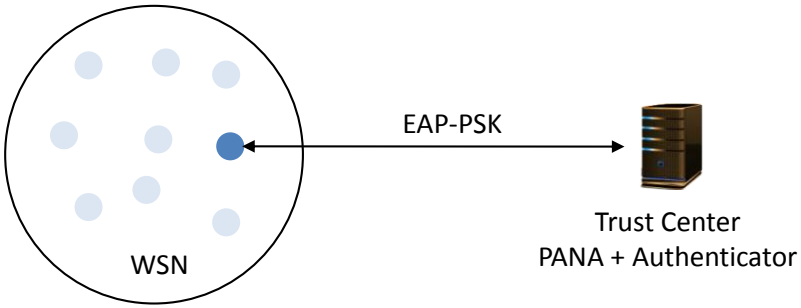


# Security Framework Module Overview

| | |
|---|---|
| Authentication | authenticate a node against a Trust Center |
| Key Management | establishment and management of key |
| Parameter Manager | centralized configuration of node parameters |
| Data Aggregation | aggregation on router nodes and the gateway |
| NWK Access Control | establish security gates in WSN |
| Security Provider | responsible for ciphering and deciphering |
| Device Update | update device firmware |
| Threat Detection | detection of threats and alerting of operators |

# Security Framework – Authentication (AM)

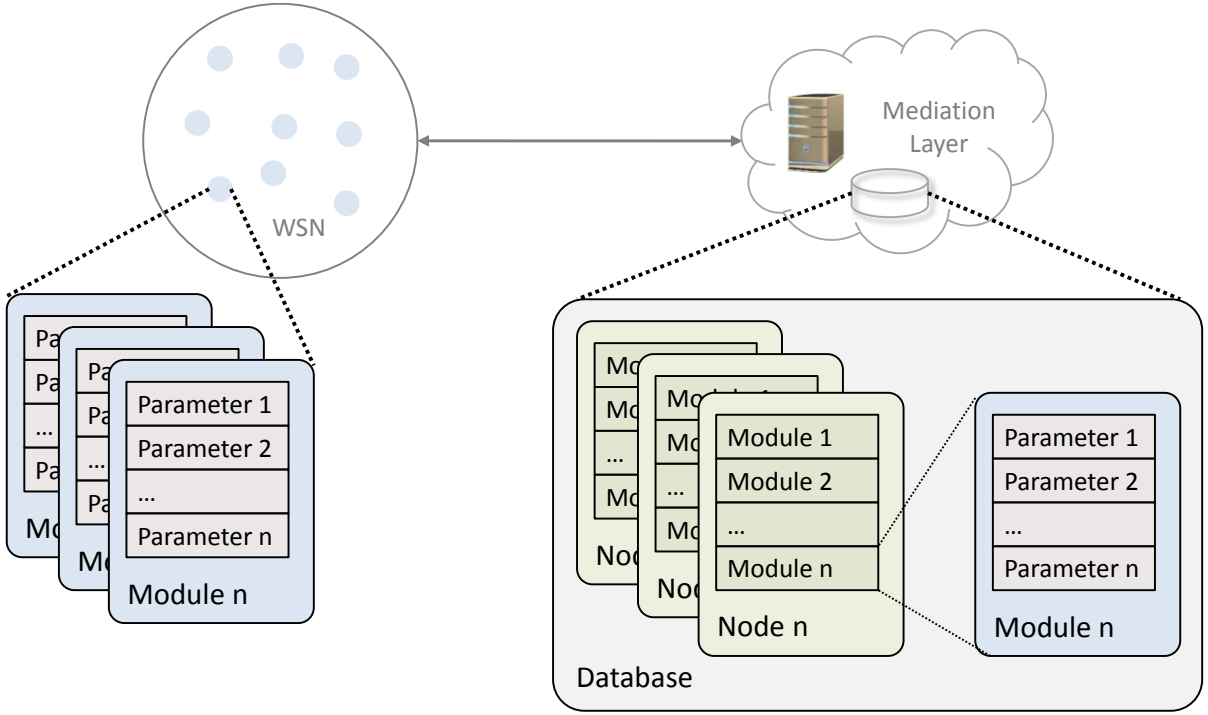
- authenticate a node against a Trust Center
- first step after node joined the WSN
- based on PANA/EAP-PSK
- based on a pre-shared secret
- as result of an successful authentication a Master Session Key is derived




- mediation layer follows two paradigms:
  - reject messages from not authenticated nodes
  - forbid business application access to not authenticated nodes
- node follows the paradigm:
  - no communication without authentication

# Security Framework – Parameter Manager (PM)

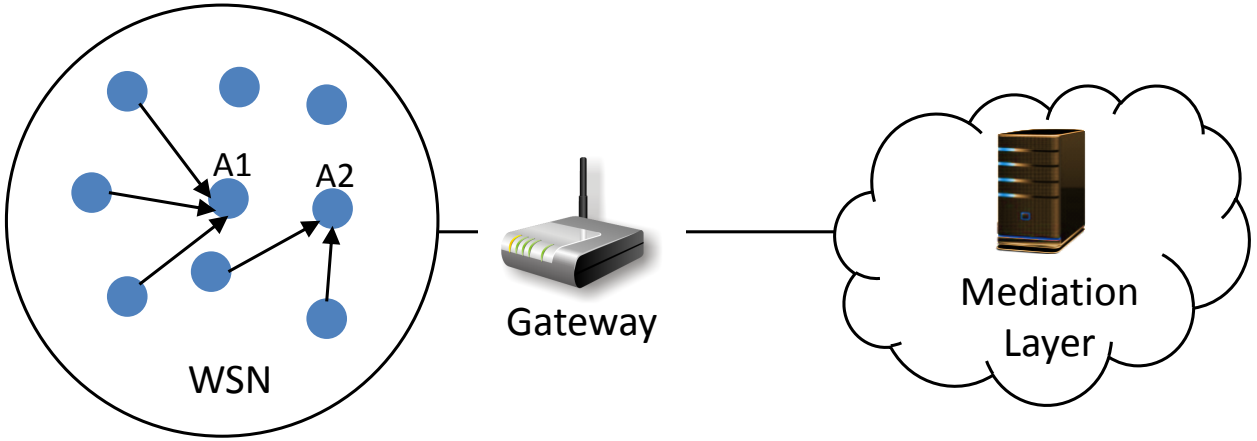
- centralized configuration of node parameters (second step after authentication)
- configures framework modules as well as node application




- allows registration of user/module parameter without itself knowing about the content (Strings, 8-Bit / 16-Bit Integers, …)
- Mediation Layer stores parameters per node in database

# Security Framework – Data Aggregation & Processing

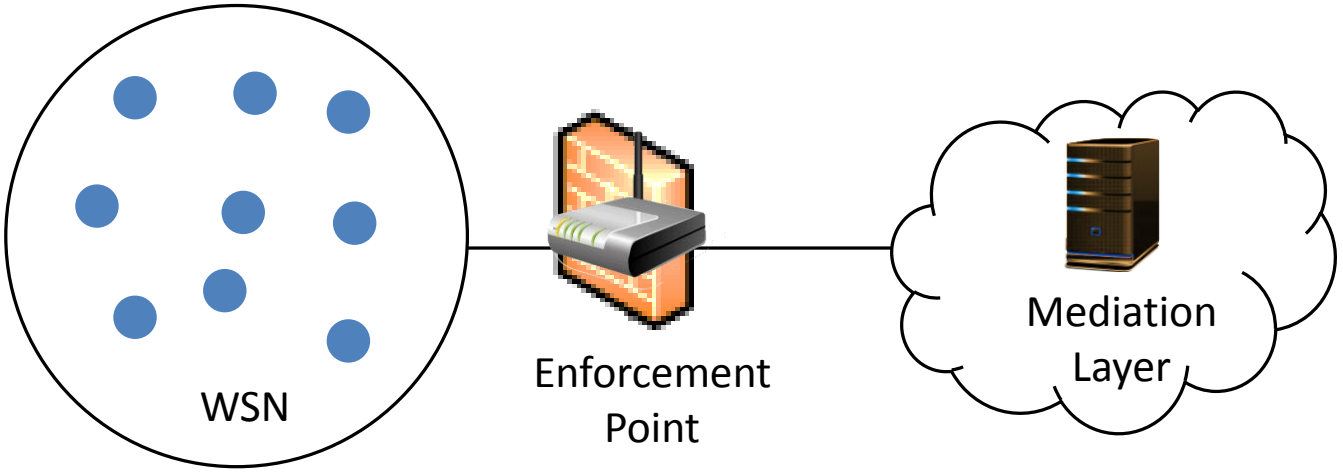
- perform aggregation on router nodes and the gateway (devices always on)
- offer an interface to user application
- application sends (measurements) to and receives (commands) from the DAP
- user application does not care about security – done by framework
- user application does not care about aggregation – done by the framework




- aggregation can be runtime configure via the mediation layer
- configured aggregator node aggregates all data from any node

# Security Framework – Network Access Control (NAC)

- establish security gates in WSN to stop malicious data as soon as possible
- each node can be configured at runtime to use NAC
- to make management simple (taking wireless routing into account) only the gateway can be chosen as enforcement point




- only legitimate nodes can send data past the gateway towards mediation layer

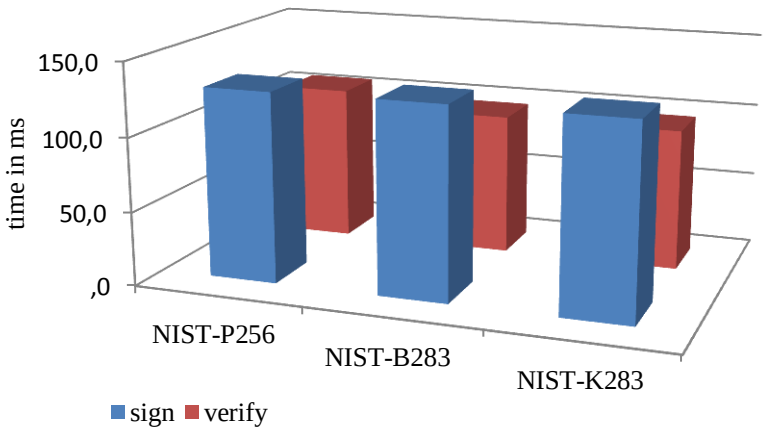
# Security Framework – Security Provider (SP)

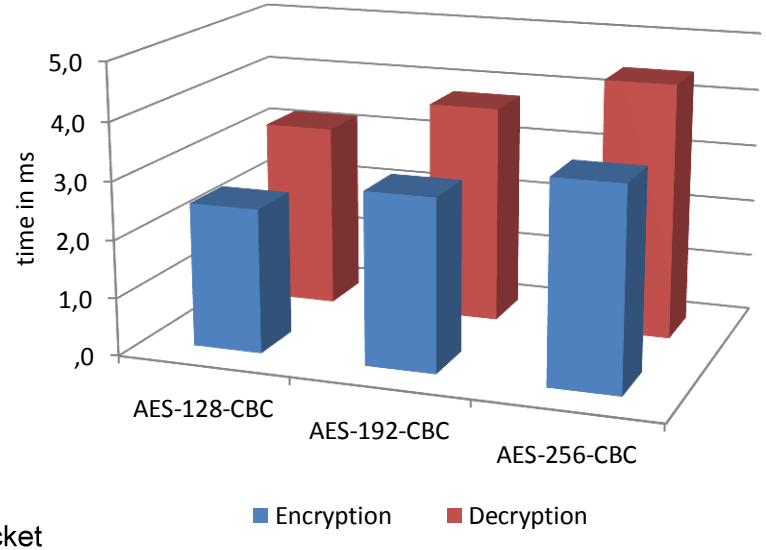
- responsible for security application and checking
- includes packet processing (in which order must security be applied when integrity check and encryption is defined)
- all modules rely on the SP for security
- only interprets the SA to process a packet
- a firmware update can update existing/introduce new algorithms

| Group | Algorithm |
|---|---|
| Hash | MD5 / SHA1 / SHA224 / SHA256 / SHA384 / SHA512 |
| HMAC | HMAC-MD5 / HMAC-SHA1<br>HMAC-SHA224 / HMAC-SHA256<br>HMAC-SHA384 / HMAC-SHA512 |
| Symmetric Cipher | AES128-CBC / AES128-ECB / AES128-CCM<br>AES192-CBC / AES192-ECB / AES192-CCM<br>AES256-CBC / AES256-ECB / AES256-CCM |
| Asymmetric Cipher | ECDSA-NIST-P256<br>ECDSA-NIST-B283<br>ECDSA-NIST-K283 |

# Security Framework – Security Provider (SP)

- all crypto operations are supported by resource constrained sensor nodes
- test with software and hardware accelerated crypto engines were done (8 bit AVR, 32 bit ARM7)
- also constrained sensor nodes can run software cryptography except ECDSA
- asymmetric cryptography can be used for data transport if a hardware accelerator is used

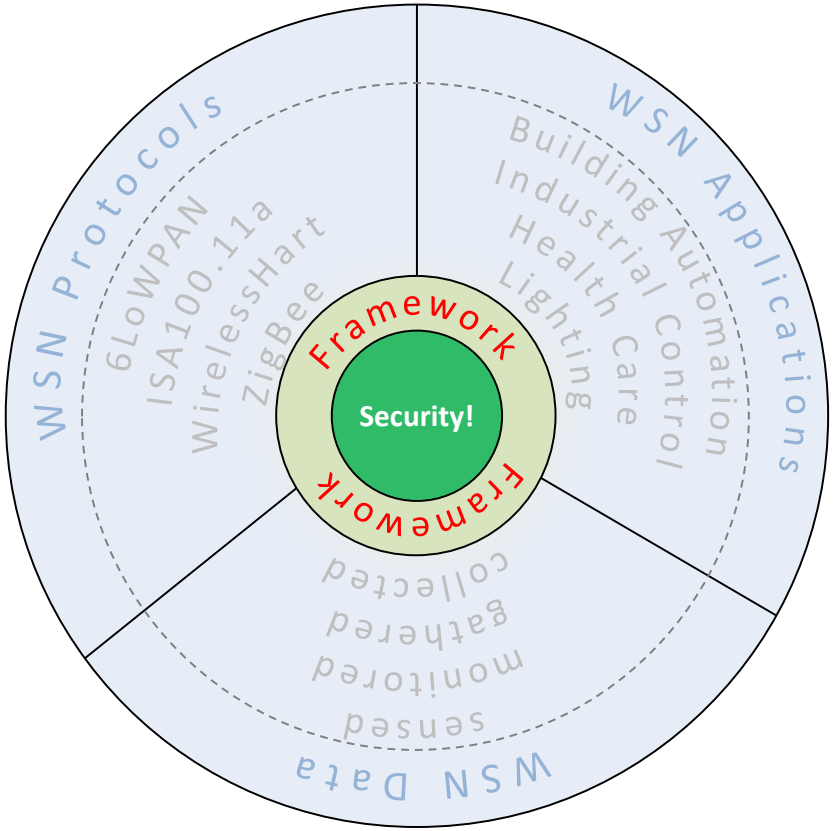



Results are shown for an 8 bit AVR at 16 MHz, 64 byte data packet

# Security Framework Conclusion

**What does the Security Framework provide?**



# Thank you for your attention!

Mike Ludwig
mike.ludwig@dresden-elektronik.de