

# Wim Bos

wbos@lumiad.nl

HTS Werktuigbouw – MBA

Philips - AT&T - Lucent Technologies – Internationale projecten

Lucent – Agere Uitvinders van WiFi

Lumiad - Lumiad Xtended Technologies

Managing High tech - Devil is in the details

Je wordt zelden overreden door een vrachtauto uit de richting waar je keek

## LUMIAD

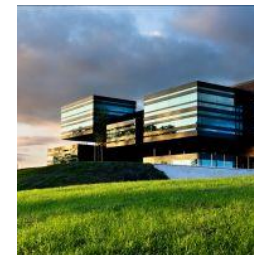
- Lucent – Agere Nieuwegein inventors Wlan – WiFi
- Reliable networking – Focus on (mission critical) networks
- Present in different markets; Wan, Lan, Wlan and RTLS (Real Time Locating System)
- Dedicated healthcare and Industrial team

## LXT – IOT HW en SW development

- Low power HW + different radio technologies
- Evresys location based services and products and IOT communication SW

## Brama XS Suite

- Cybersecurity product – Identity and Authentication Consolidation

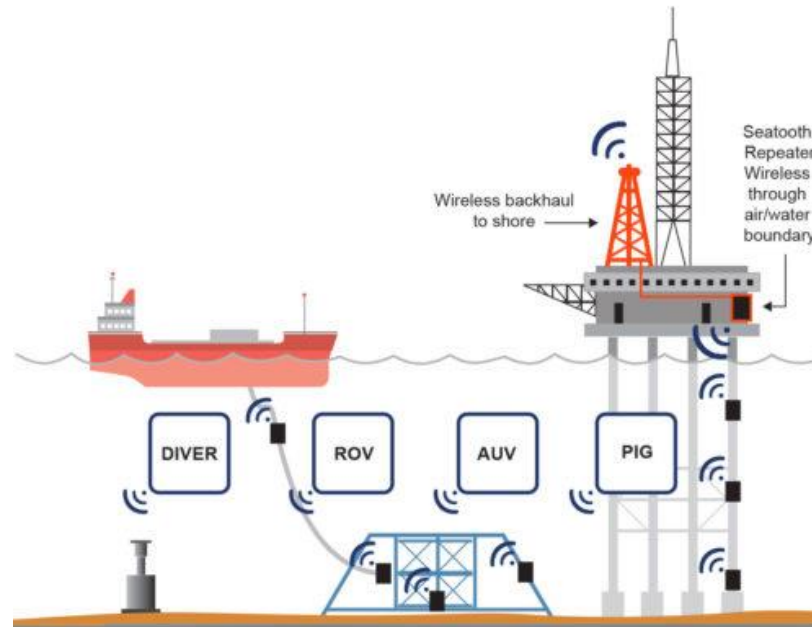


# ***Cyber security Internet of Things – driver***

*Standalone Items now connected*

*New applications*

- Connectivity - Private LTE (nbiot) – WiFi – Lora – BLE
- Data security – VPN - Encrypted point to point
- Augmented reality



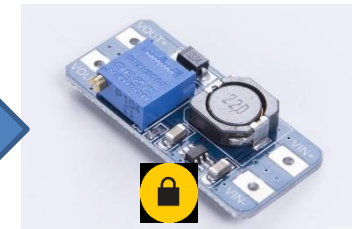
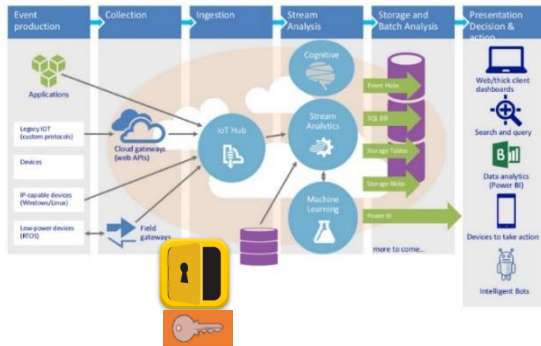
# IOT Building Blocks

## Manage complete chain

Central cloud

(Micro) Edge equipment

IoT Application Pattern



IOT "School"

"intelligence" in the cloud versus

"intelligence" at the "edge" – distributed intelligence

# ***Cyber security – Control of Complexity***

- Embedded in the organization - Ease of use
- Design - Failure Mode and Effect Analysis
  - Design for reliability =/+ Design for security
    - Technology can cq will fail – Organizational backup plan
    - User must be able to see if system is secure or reliable
- Technical Management
  - Management and monitoring
  - Redundant design – Reliability

Design for Security = Design for reliability

CIA Principle – Confidentiality, Integrity and Availability

# ***IOT – Equipment identity and Integrity***

Positioning Paper Fraunhofer Institute: [Geräteidentität und -integrität im Internet der Dinge](#)

## Requirements

- Reliability of the Equipment – Data Protection – Scalability – Availability

Single Equipment identity = Equipment - identity & Integrity =

- Hardware identity – processor # - Safe storage with certificate (special chip)
- Software identity – Used over different devices PKI to identify software integrity
- Operational parameters - settings– central management – distributed intelligence

Manage - Hardware - Software - Access

Identity via PKI Electronic Certificates

<http://imediman.ifak.eu/de/content/ger%C3%A4teidentit%C3%A4t-und-integrit%C3%A4t-im-internet-der-dinge>

[https://www.sit.fraunhofer.de/fileadmin/dokumente/studien\\_und\\_technical\\_reports/Taskforce-Trusted\\_Computing\\_Positionspapier\\_201704\\_einseitig-web.pdf?\\_=1492672569](https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Taskforce-Trusted_Computing_Positionspapier_201704_einseitig-web.pdf?_=1492672569)

# ***Cyber security – Important Standards***

## **ISO 27000 – ISO 27001 Data security**

- Access and control of the systems - networks
- Procedures in place for security process – Who – What - Responsibilities

## **IEC 62443-2-4:2015 - Cyber security**

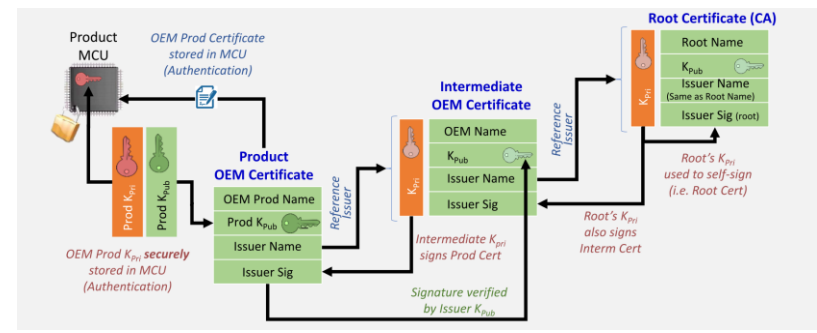
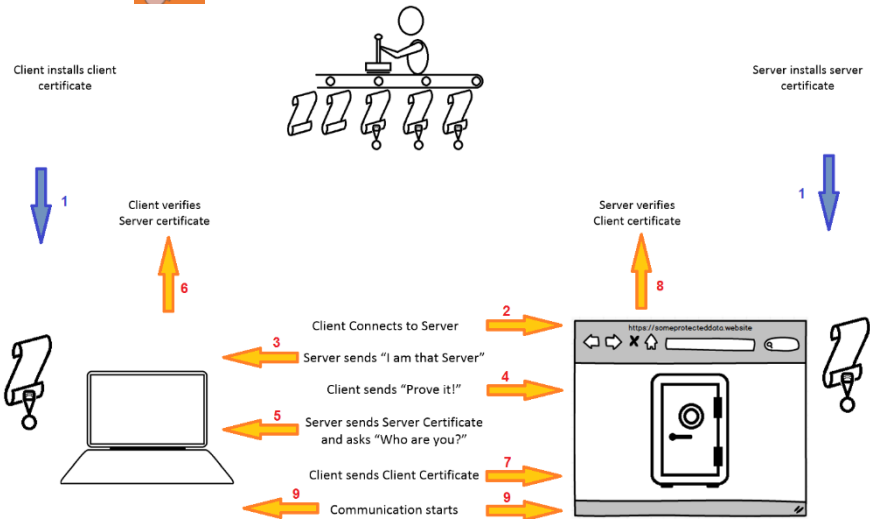
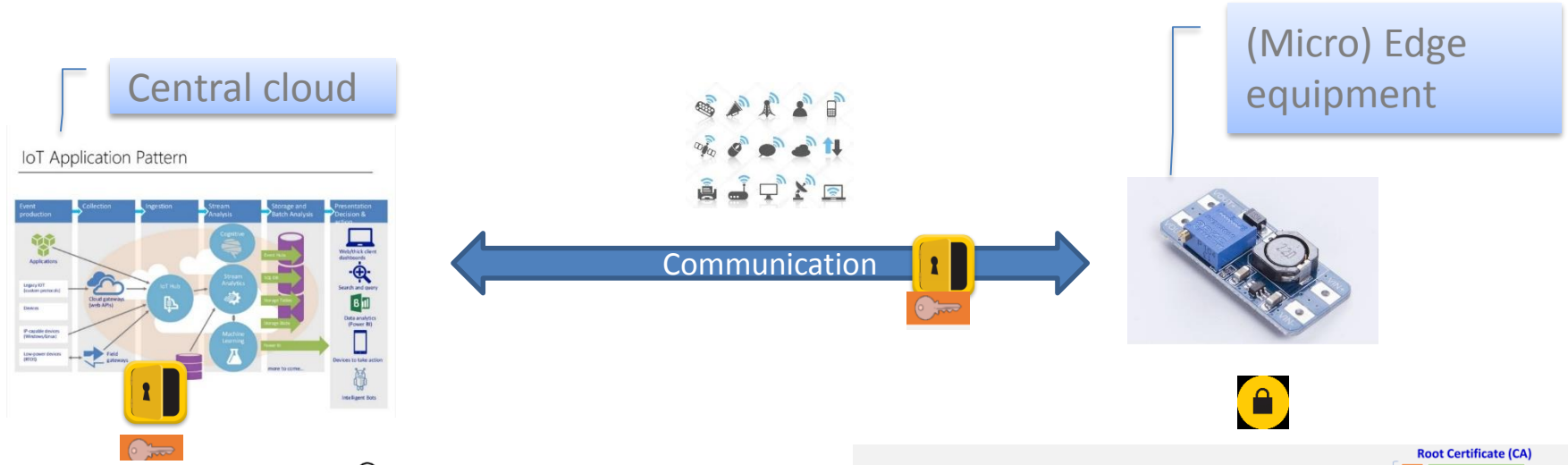
- Technical and operational requirements Hardware – Software
  - Hardened operating system
  - Central control and updates
  - Easy configuration – Can not make “mistakes” – Human failure

Manage - Hardware - Software - Access

Identity via PKI Electronic Certificates

# IOT Building Blocks

Reliable and Secure – Manage complete chain of PKI

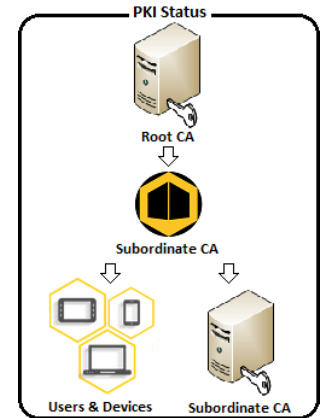




# ***BramaXS – KMS – PKI distribution + Access (SDN)***

Brama XS Suite, is identity – PKI distribution and Access control engine

- Provide access to networks and applications
- Highest level of security based on PKI ;
  - Built-in 1, 2 or 3 - tier PKI + Management
- Basis for:
  - Software Defined Access
  - Basic for machine and Server access
  - Machine – SW - Identity
  - IOT (Key lock system) – Application access etc
    - Connected
    - Standalone



# PKI distribution and Use - Make it easy to use

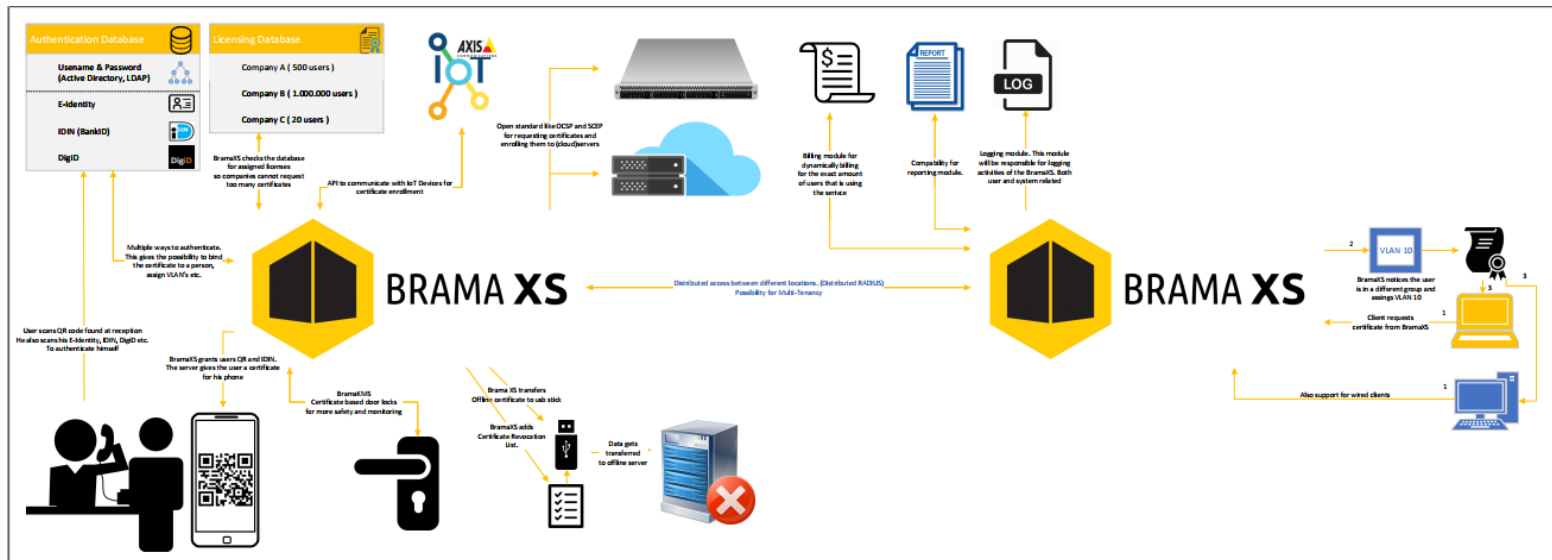
Combination of Functions – Access to network = access to building

Three factor authentication -

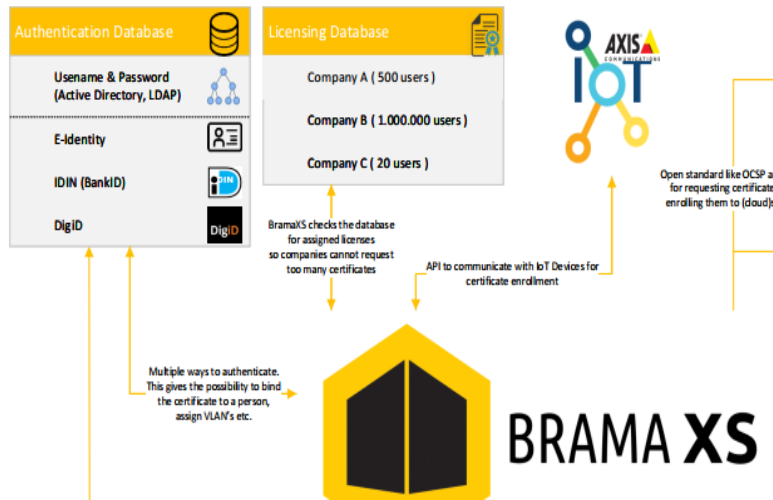
What you have - Smartphone + fingerprint - TicTac (location)

What you know – Password – Pincode

What you are – PKI combined with identity (idin – passport etc)



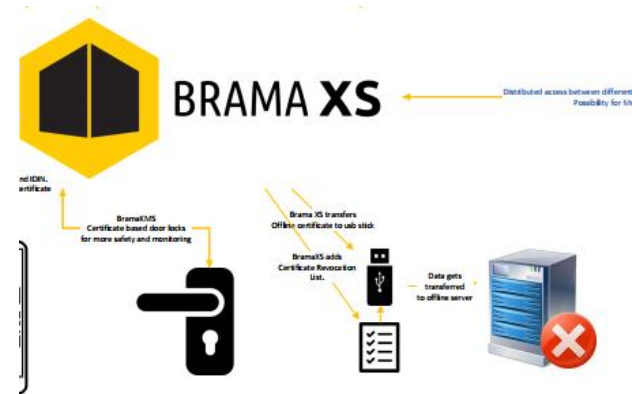
# BramaXS /KMS / IOT



## Identity generation Side A

### Check Identity – Provide PKI

- Username – PW
- E identity (IDIN=bankaccount check)
- Simple QR scan
- Automated rollout for hardware



## Identity check on Side B - Access

### Check Identity via PKI – Provide access

- PKI + Username – PW
- PKI + E identity (IDIN=bankaccount check)
- PKI + double human check

## Standalone capabilities

# ***Cyber security – Existing equipment***

## **Existing equipment –**

- Security typical for reliability
- Limitations on hardware and Software

## **PKI and Secure access**

- Limitations on processing power and capabilities
  - public and private part certificate – Read out public part with text
  - External identity and encryption unit
- Secure access Limitations no WPA Enterprise
  - WPA Kiosk – Wlan and wired secure access

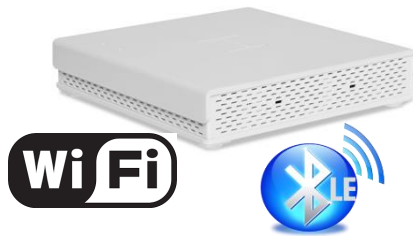


# IOT – Communication Trends ICT - IOT

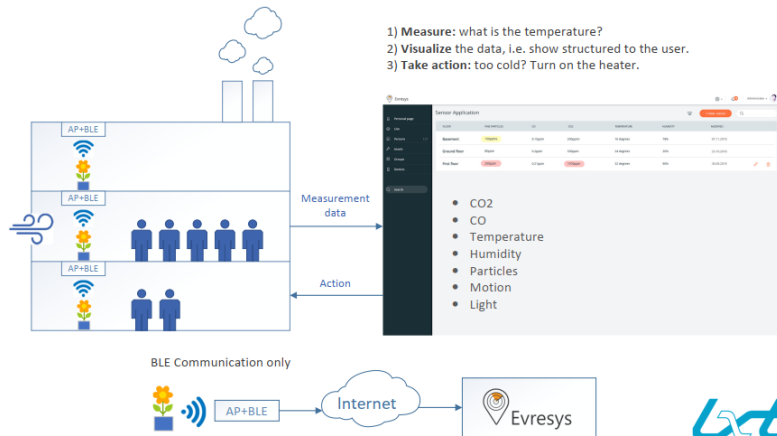
Outdoor -



Indoor -



First Product "Sensing Flowerpot": Improve your Air Quality



**wbos@lumiad.nl**