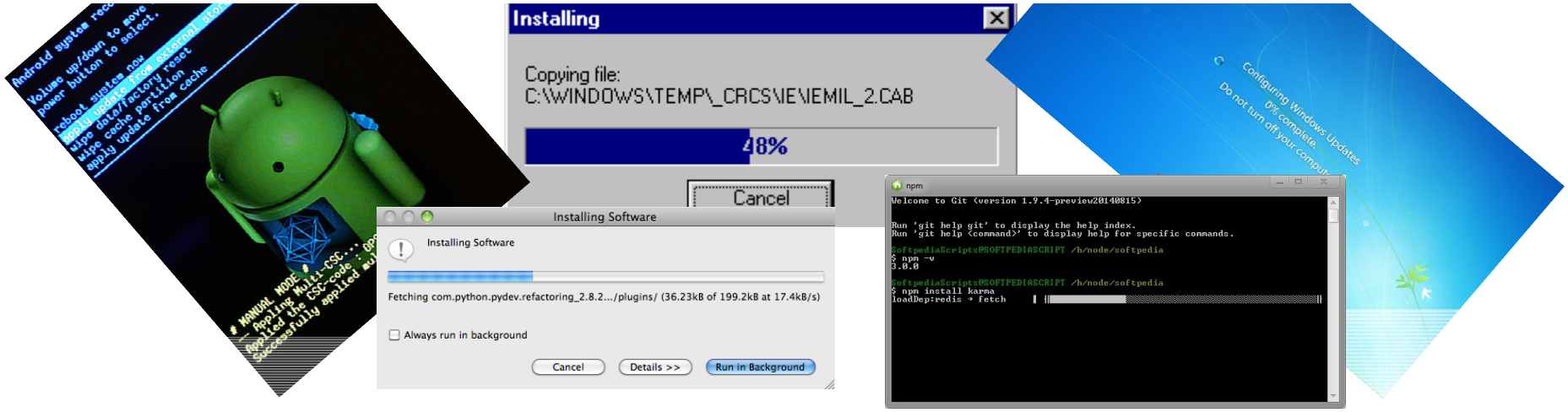
CENTRAL OFFICE OF MEASURES (GUM)
INTERDISCIPLINARY METROLOGY DEPARTMENT
SOFTWARE RESEARCH AND TESTING LABORATORY

Mosiadz Michal, Puchalski Jacek,
Szelagowski Pawel, Wojcik Jacek

METHODS OF SOFTWARE UPDATE SECURING IN MEASUREMENT DEVICES



3RD WORKSHOP „SOFTWARE AND ICT RELATED CHALLENGES IN LEGAL METROLOGY
BERLIN 21ST – 22ND JUNE 2017

METHODS OF SOFTWARE UPDATE SECURING IN MEASUREMENT DEVICES

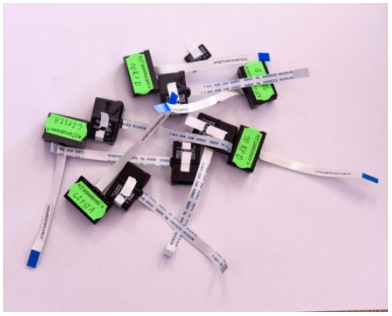
AGENDA

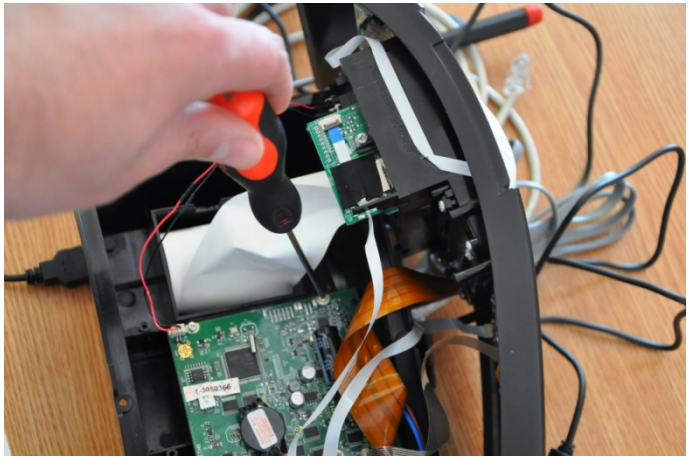
- ABOUT US
- SOFTWARE UPDATE REQUIREMENTS
- SOFTWARE UPDATE PROCESS
- UPDATE SECURING METHODS
  - PHYSICAL SEALING
  - PASSWORDS
  - ACCESS LEVEL
  - ELECTRONIC SIGNATURE
  - VERSION COMPARISON
  - LOCAL / ONLINE UPDATE
  - PHYSICAL LIMITATION OF ACCESS TO UPDATES
- NON-LEGAL RELEVANT UPDATES
- PREFERABLE SOLUTIONS
  - PHYSICAL SEALING
  - PASSWORDS
- RISKS
- FUTURE ?

Central Office of Measures (GUM) - POLAND

METHODS OF SOFTWARE UPDATE SECURING IN MEASUREMENT DEVICES

SOFTWARE RESEARCH AND TESTING LABORATORY



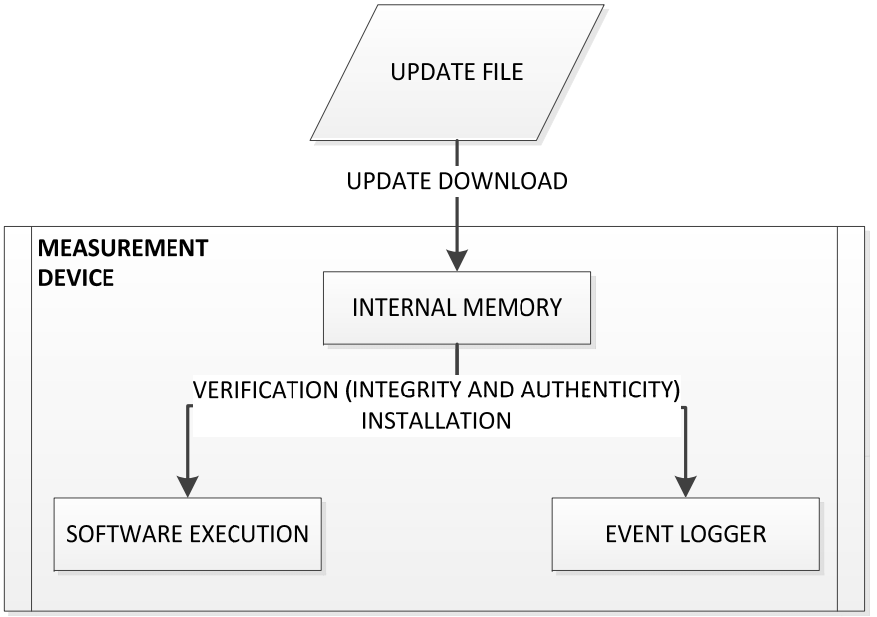


3RD WORKSHOP „SOFTWARE AND ICT RELATED CHALLENGES IN LEGAL METROLOGY
BERLIN 21ST – 22ND JUNE 2017

SOFTWARE UPDATE RESTRICTIONS

WELMEC WG7.2 - EXTENSION D
DOWNLOAD OF LEGALLY RELEVANT SOFTWARE

- D1: DOWNLOAD MECHANISM
- D2: AUTHENTICATION OF TRANSMITTED SOFTWARE
- D3: INTEGRITY OF DOWNLOADED SOFTWARE
- D4: TRACEABILITY OF LEGALLY RELEVANT SOFTWARE DOWNLOAD

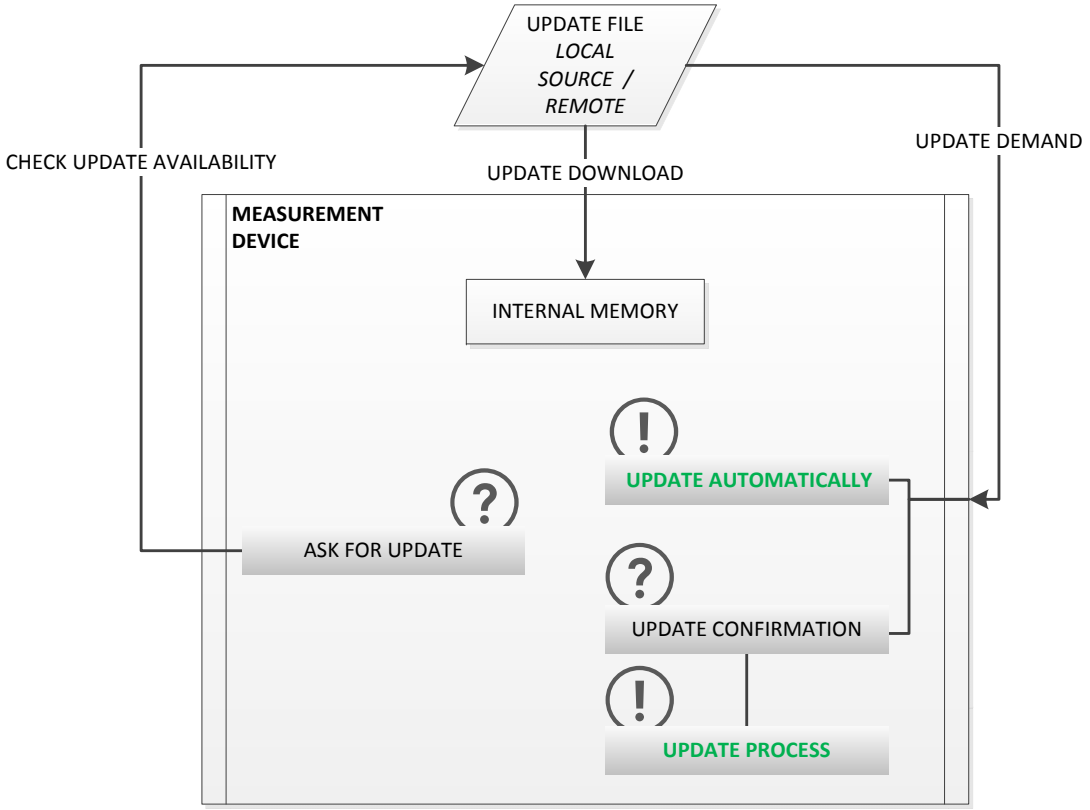


SOFTWARE UPDATE PROCESS

DOWNLOAD ACTIVATION

D1

- AUTOMATIC / ON DEMAND
- PROCESS CONFIRMATION



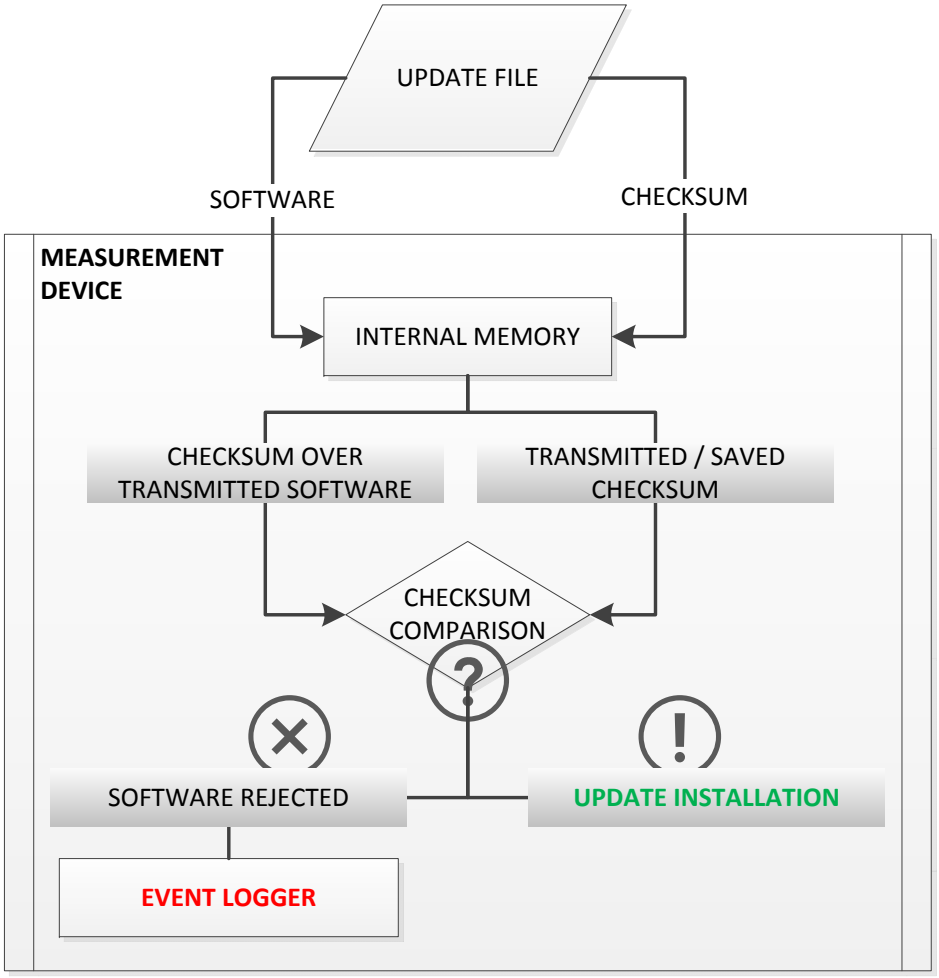
SOFTWARE UPDATE PROCESS

TRANSMISSION VERIFICATION

D1, D3

- CHECKSUM / ELECTRONIC SIGNATURE VERIFICATION
- TRANSMITION ERRORS
- DATA CHANGES DURING TRANSMISSION

INSTALLATION FORBIDEN
SOFTWARE REJECTED



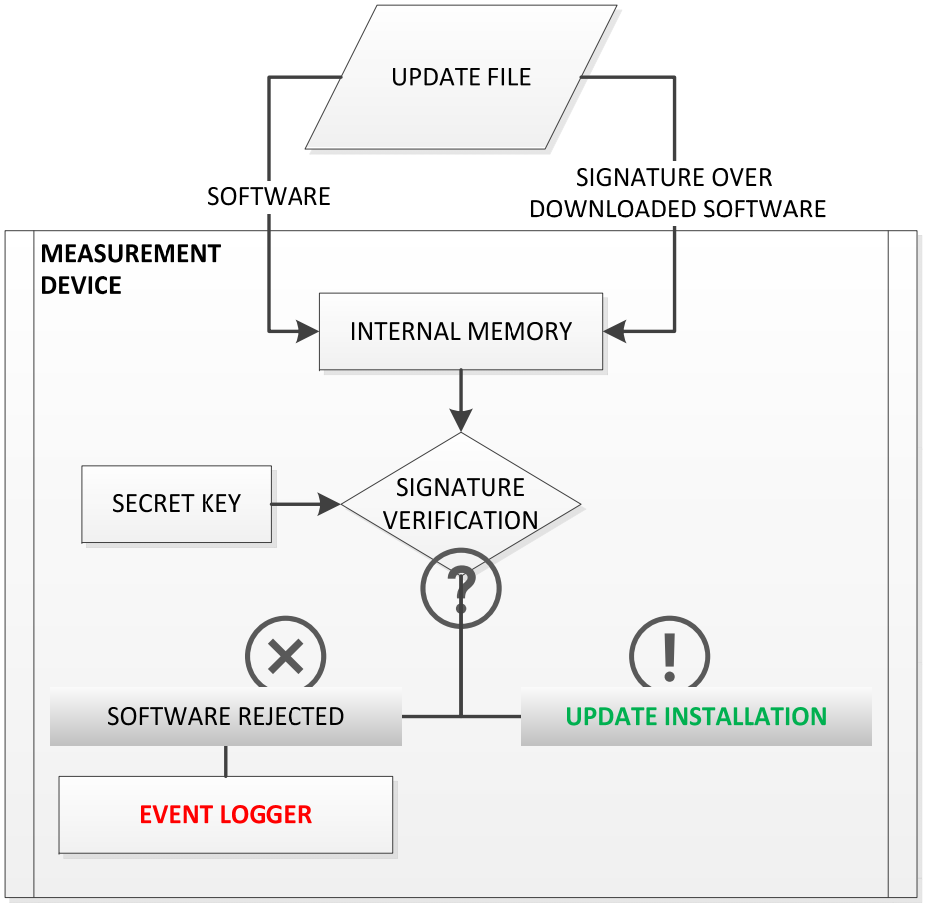
SOFTWARE UPDATE PROCESS

AUTHENTICITY OF SOFTWARE

D1, D2

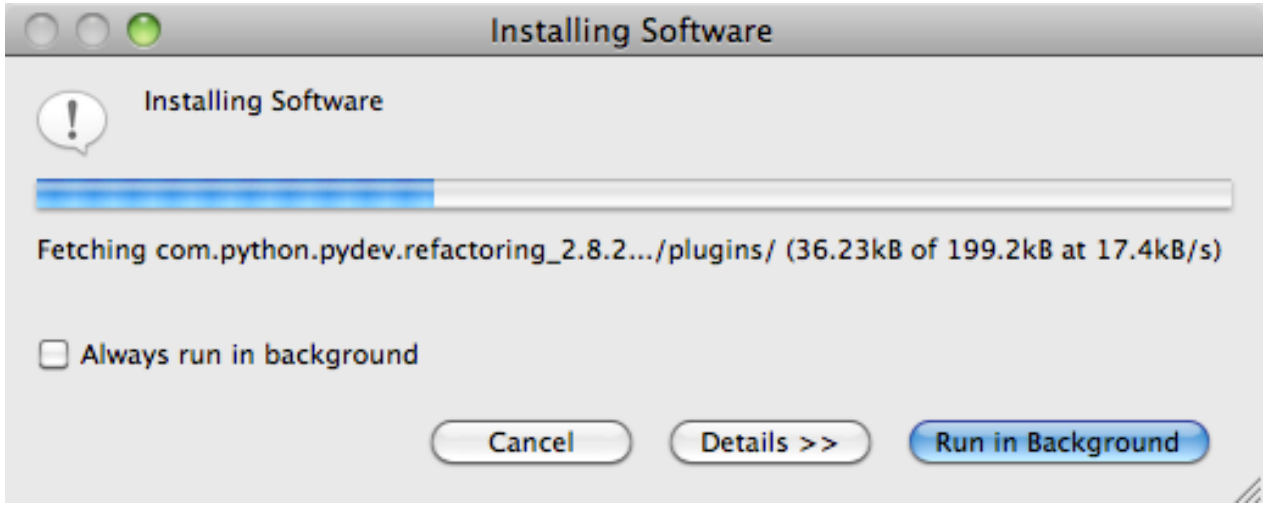
- ELECTRONIC SIGNATURE VERIFICATION
  - MANUFACTURER SIGNATURE
  - NB SIGNATURE
- COMPATIBILITY VERIFICATION

INSTALLATION FORBIDEN
SOFTWARE REJECTED



SOFTWARE UPDATE PROCESS

UPDATE INSTALLATION / EXECUTION

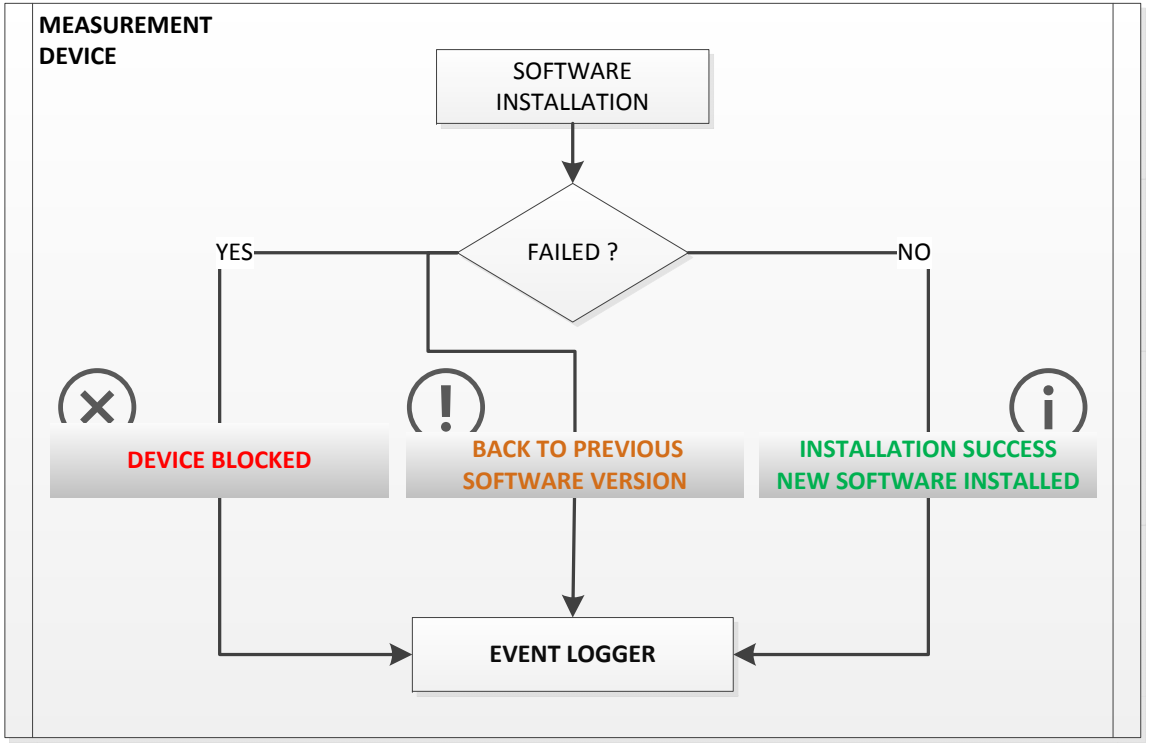


SOFTWARE UPDATE PROCESS

INSTALLATION VERIFICATION
SOFTWARE TRACEABILITY

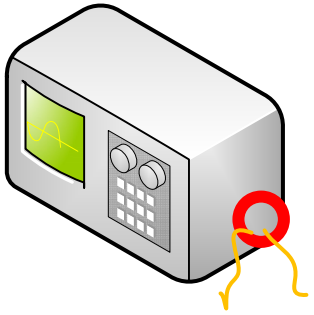
D1, D3, D4

- INSTALLATION FAILS
  - DEVICE BLOCKED
  - RETURN TO PREVIOUS SOFTWARE VERSION
- TRACEABILITY
  - EVENT LOGGER

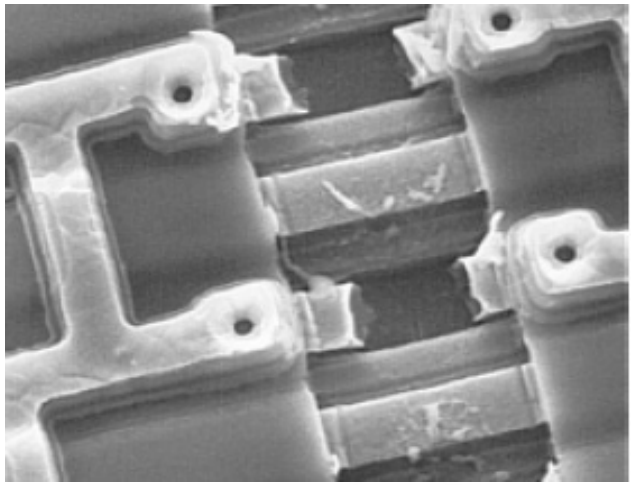


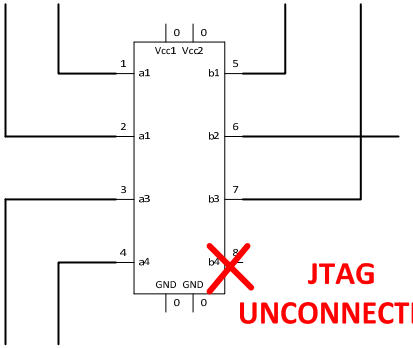
SOFTWARE UPDATE SECURING

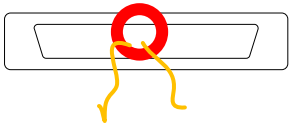
PHYSICAL SEALING



DEVICE SEALING







ADDITIONAL COMMUNICATION PORTS SEALING

METHODS OF SOFTWARE UPDATE SECURING IN MEASUREMENT DEVICES

SOFTWARE UPDATE SECURING

MINIMAL REQUIREMENTS

NO UPGRADE POSSIBILITY WITHOUT BREAKING SEALING

ADDITIONAL SECURING METHODS

- HARDWARE SERVICE MODE TOOLS (LIMITED ACCESS)
- - SPECIAL SERVICE PASSWORDS
- SERVICE JUMPER WITH ADDITIONAL SEALING
- REQUIRED ACCESS TO UPDATE FILE

EVENT LOGGER

METHODS OF SOFTWARE UPDATE SECURING IN MEASUREMENT DEVICES

SOFTWARE UPDATE SECURING

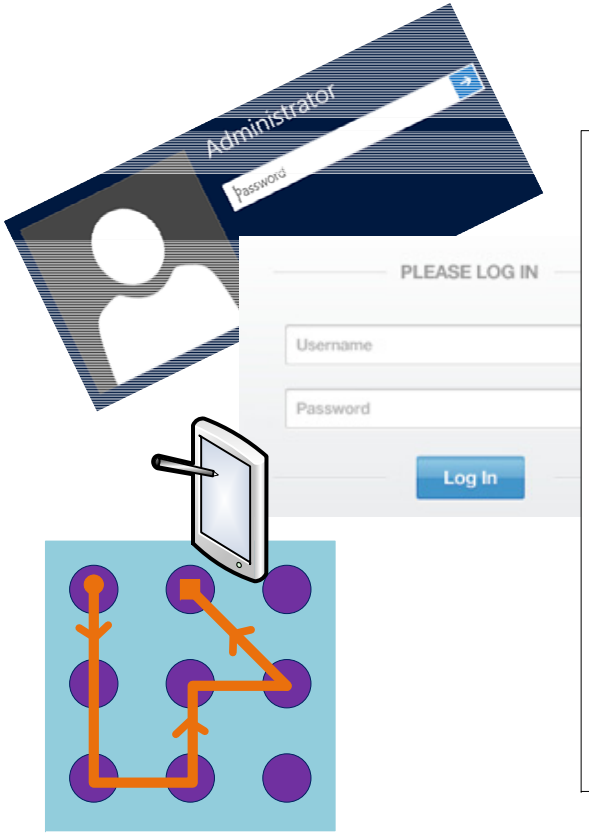
PHYSICAL SEALING

1. Service jumper
2. Program saved in OTP memory.
3. Hardware key

METHODS OF SOFTWARE UPDATE SECURING IN MEASUREMENT DEVICES

SOFTWARE UPDATE SECURING

ACCESS ACCOUNTS
PASSWORDS AND AUTHORISATION TOOLS
„SECRET" BUTTON CODE



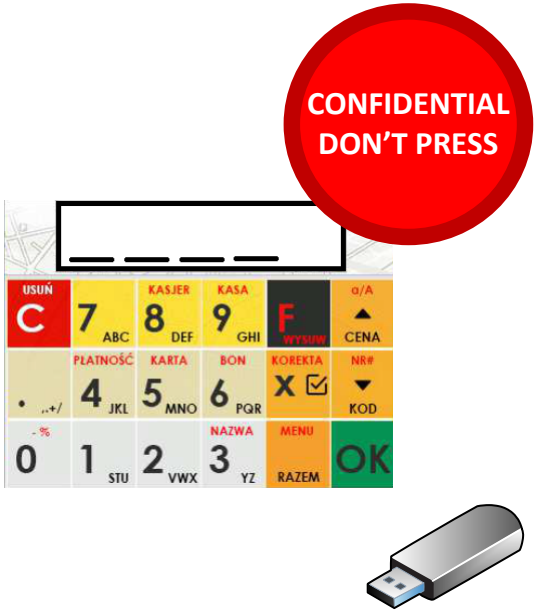
USER ACCOUNTS
ACCESS LEVELS

USER

SERVICE

ADMIN

CLIENT



TECHNICAL REQUIREMENTS
OR
SECURITY AUDITS
???

METHODS OF SOFTWARE UPDATE SECURING IN MEASUREMENT DEVICES

SOFTWARE UPDATE SECURING

NEW APPROACH

ONLINE SOFTWARE UPDATE WITHOUT BREAKING PHYSICAL SEALING

SECURING METHODS

EVENT LOGGER
ELECTRONIC SEALING
LIMITED ACCESS TO UPDATE FILE AND AUTHORISATION TOOLS

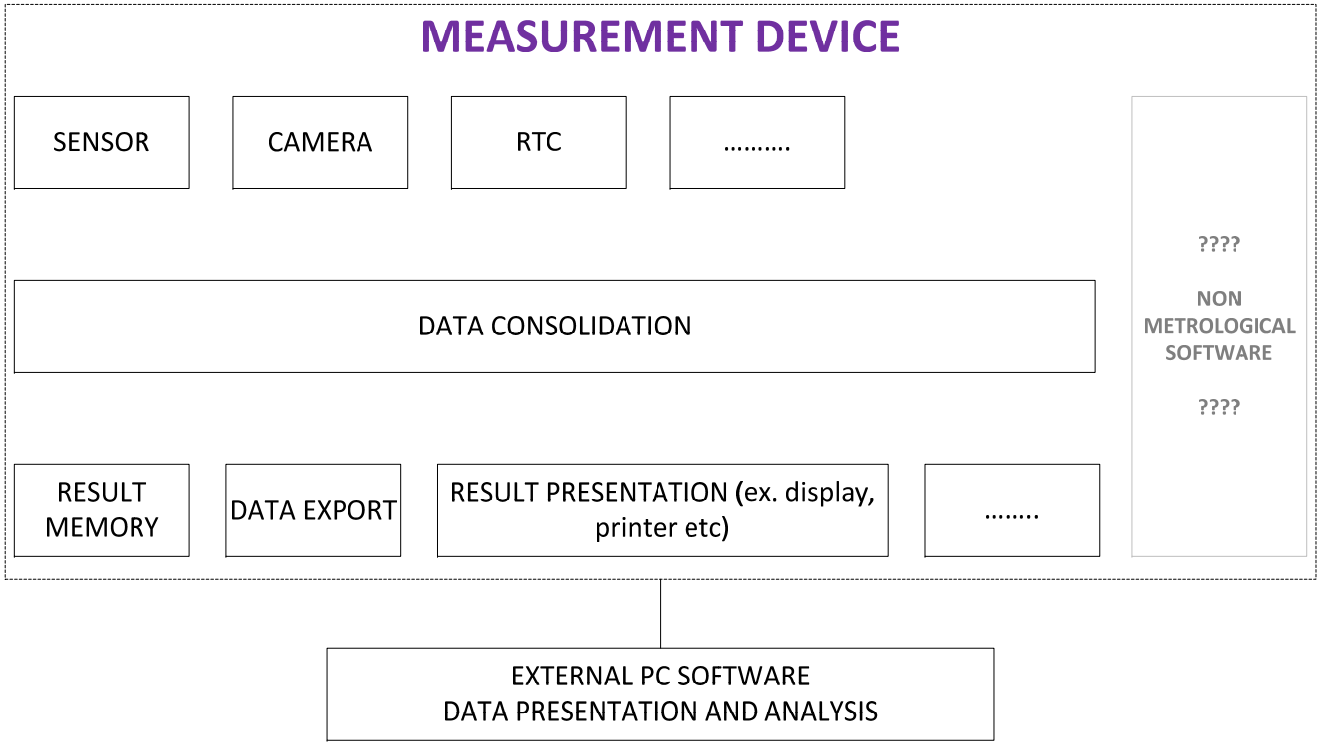
- ACCESS TO SERVICE MODE – ELECTRONIC KEY
- AUTOMATIC UPDATE TRANSMISSION, SIGNALISATION FOR USER
- UPDATE MOMENT CONFIRMATION
- MULTIPLE VERIFICATION OF UPDATE STAGES SUCCESS

REQUIRED CHANGES IN LAW – AUDIT OF MANUFACTURES QUALITY SYSTEM ???
(SEE: SWEDISH LAW FOR CASH REGISTERS)
TECHNICAL OR ORGANISATIONAL PROBLEM ???

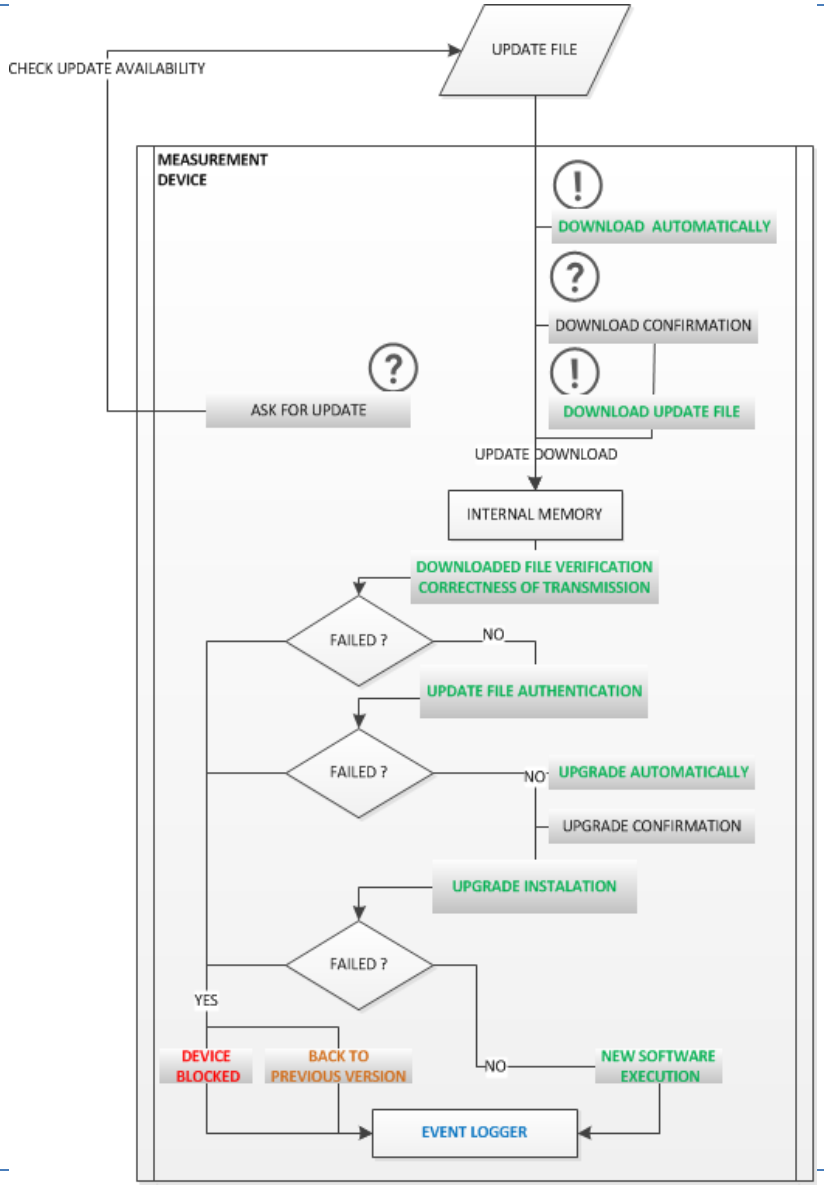
METHODS OF SOFTWARE UPDATE SECURING IN MEASUREMENT DEVICES

SOFTWARE UPDATE SECURING

NON-LEGALLY RELEVANT UPDATES



METHODS OF SOFTWARE UPDATE SECURING IN MEASUREMENT DEVICES



SOFTWARE UPDATE SECURING

PREFERABLE SOLUTION

ALGORITHM DEVELOPED
FOR NEW REQUIREMENTS
FOR CASH REGISTERS IN POLAND

1. SOFTWARE DOWNLOAD
2. FILE TRANSMISSION VERIFICATION
3. UPDATE FILE AUTHENTICATION
4. CHECK FOR VALID CERTIFICATION FOR NEW VERSION
5. SOFTWARE INSTALLATION
6. EVENT LOGGER

THANKS FOR ATTENTION

mailto: ecr@gum.gov.pl