# VE-ASCOT

## Remote Attestation with Hardware Fingerprinting

Velektronik

GEFÖRDERT VOM

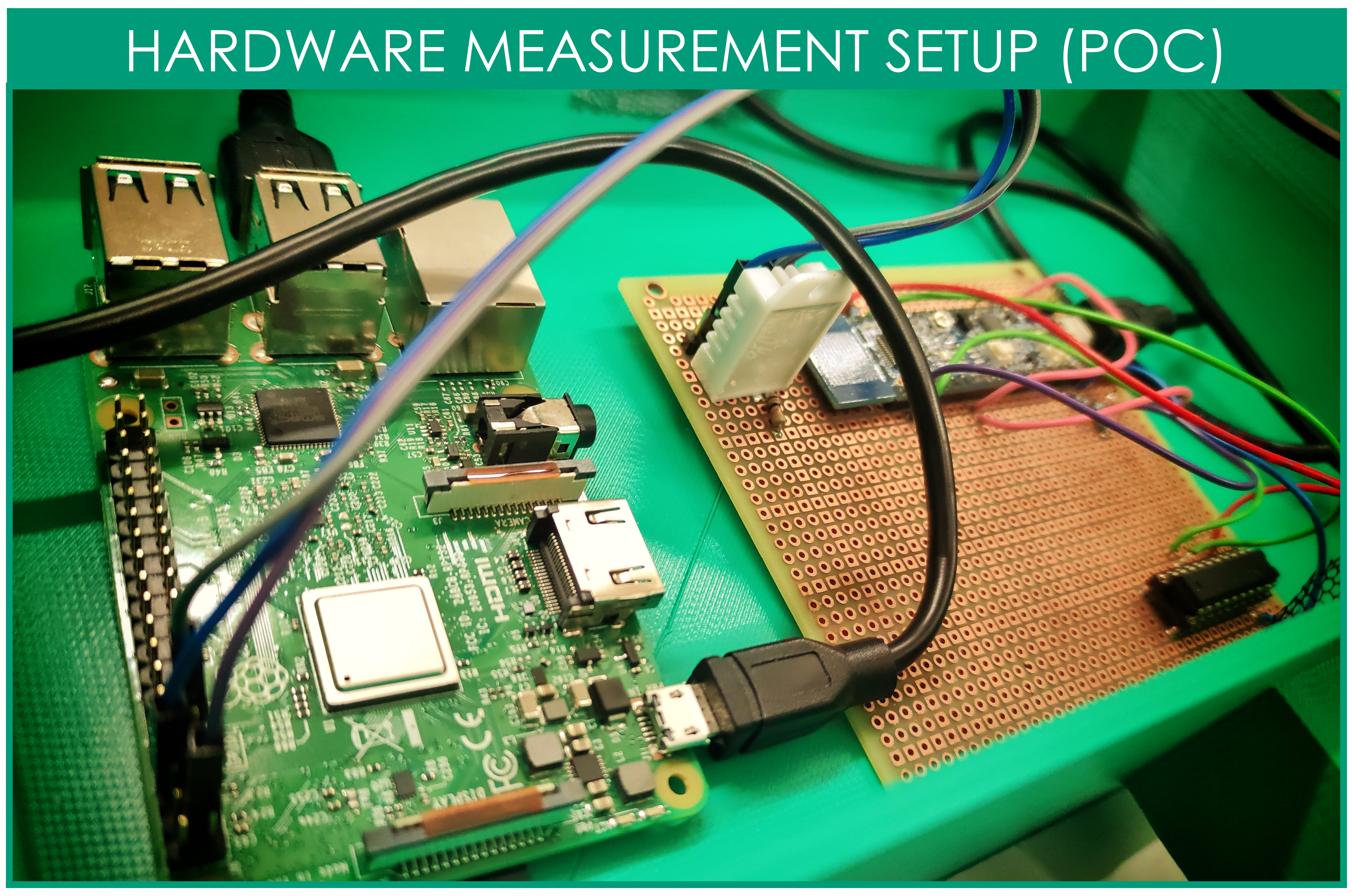
Bundesministerium für Bildung und Forschung

03/2021 – 12/2024

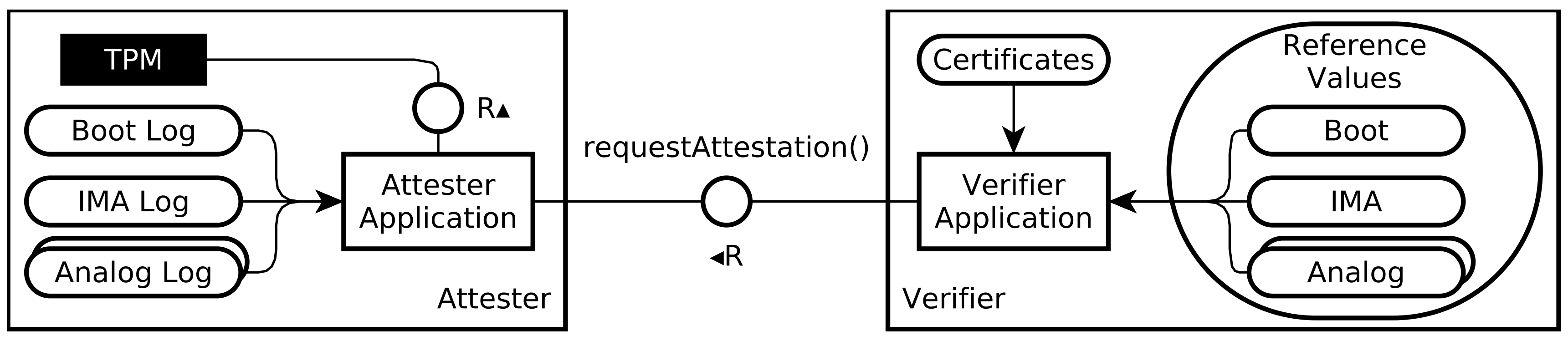
## PROBLEM

- **Complex distributed production processes** of electronic assemblies involve multiple manufacturers worldwide.
- **Trust in manufacturers** plays an important role in the production of high-quality components:
  **manufacturing quality** **functionality** **integrity**
- **Attacks on the supply chain** are possible, especially the replacement of electronic components.
- **A unique identity** of electronic components is lacking, which would make replacements detectable.
- **Compromise of hardware** components cannot be detected with state-of-the-art attestation techniques.

## HARDWARE MEASUREMENT SETUP (POC)



## ENHANCED TPM 2.0 REMOTE ATTESTATION



## LOG FORMAT FOR ANALOG MEASUREMENTS

```
AnalogMeasurement = [
  version-tag: uint, ; version of the format specification
  start-time: Time,
  measurements: [ * MeasurementSeries ]
]

MeasurementSeries = (
  target: Target,
  ?env-params: [ * NameValuePair ],
  ?start-time: Time,
  unit: Unit,
  unit-multiple: UnitMultiple,
  measurements: RegularMeasurementSeries
             // IrregularMeasurementSeries,
)

RegularMeasurementSeries = {
  values ⇒ [ * NumericalValue ],
  interval-frequency-duration,
}

IrregularMeasurementSeries = [ * (
    current-time: Time,
    NumericalValue,
  ),
]
…
```

```
Time = [
  seconds: uint / float,
  unit-mult: UnitMultipleSi,
]

Frequency = [
  hertz: uint / float,
  unit-multiple: UnitMultipleSi,
]

NumericalValue = (
  value: int / float,
)

Unit = &(
  UNIT_UNDEFINED : 0,
  UnitElectricalSi,
) ; EXTENSION POINT for future units

UnitElectricalSi = &(
  UNIT_ELECTRICAL_SI_NONE        : 1,
  UNIT_ELECTRICAL_SI_VOLTAGE     : 2,
  UNIT_ELECTRICAL_SI_CURRENT     : 3,
  UNIT_ELECTRICAL_SI_RESISTANCE  : 4,
  UNIT_ELECTRICAL_SI_CONDUCTANCE : 5,
  UNIT_ELECTRICAL_SI_CAPACITANCE : 6,
  UNIT_ELECTRICAL_SI_CHARGE      : 7,
  UNIT_ELECTRICAL_SI_INDUCTANCE  : 8,
  UNIT_ELECTRICAL_SI_POWER       : 9,
  UNIT_ELECTRICAL_SI_IMPEDANCE   : 10,
  UNIT_ELECTRICAL_SI_FREQUENCY   : 11,
)
…
```

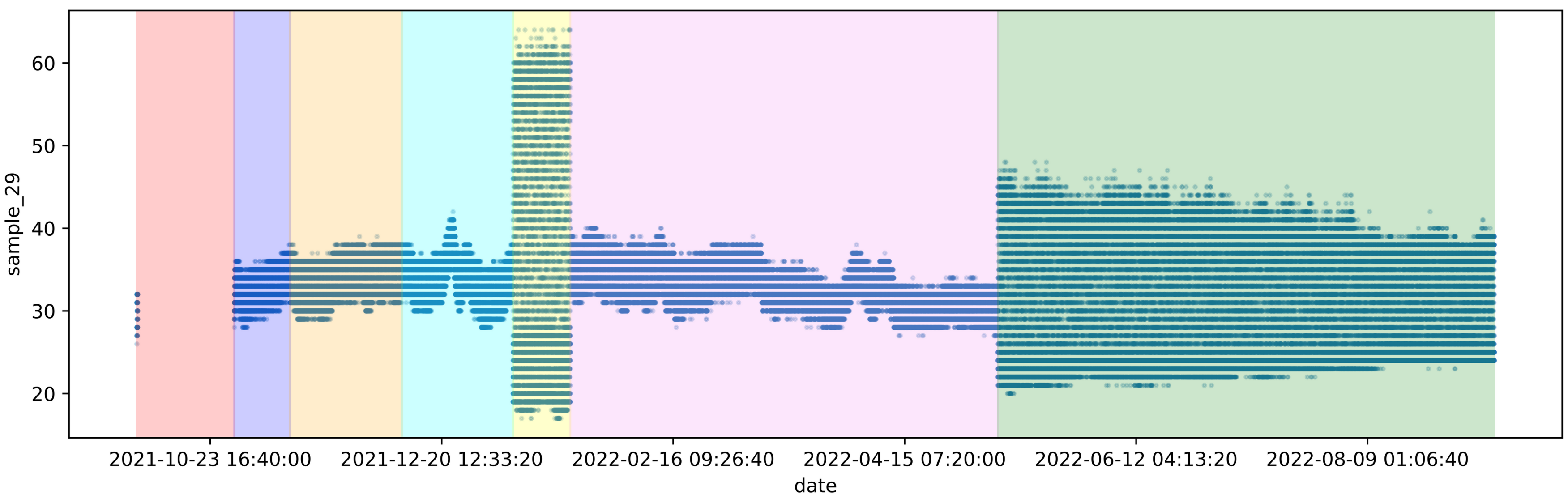
Concise Data Definition Language (CDDL); RFC 8610

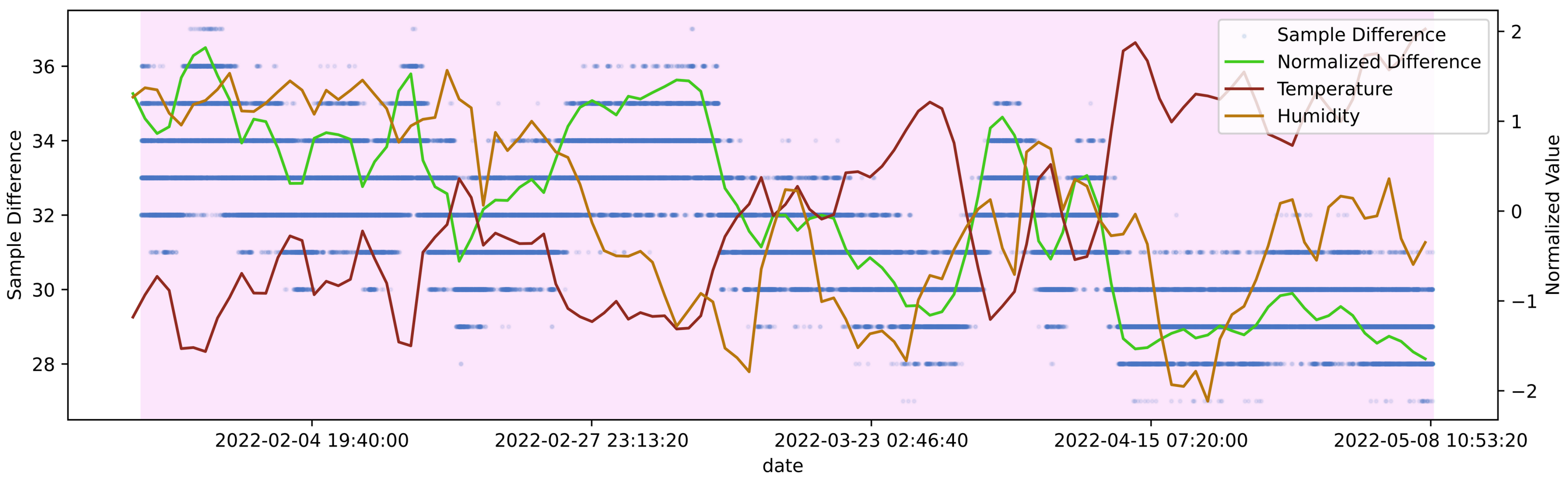
## APPROACH

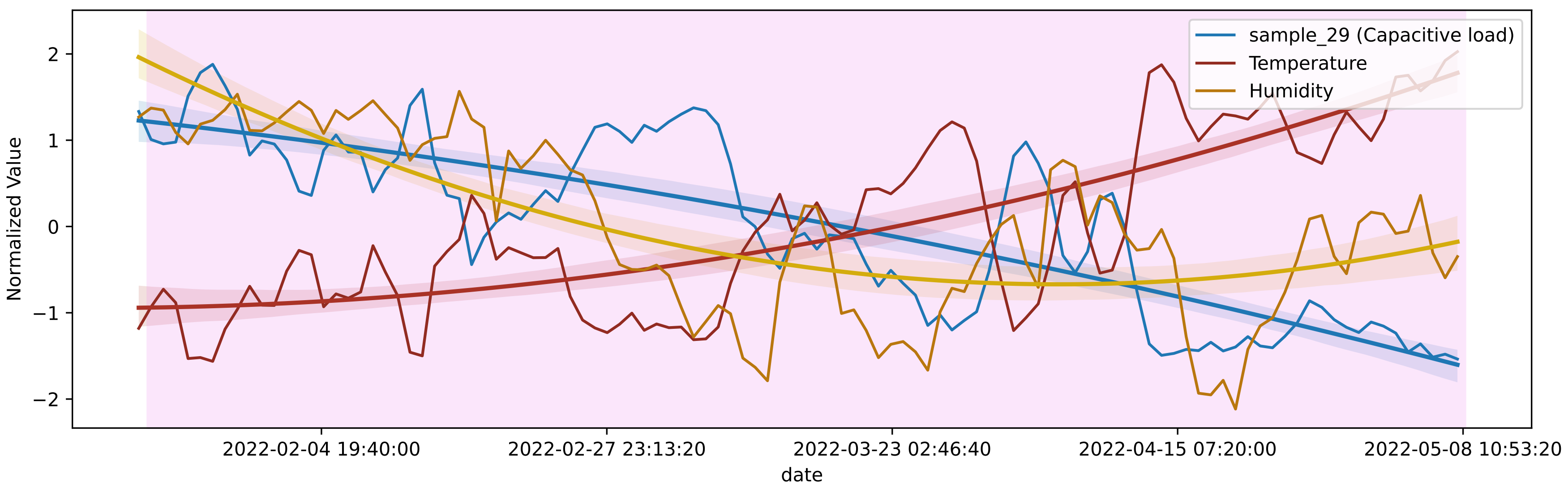
- **Identify**, **measure**, **digitize**, **process**, and **classify** unique analog **hardware characteristics**.
- Put **fingerprints into chain of trust** during production.
- **Verify** during commissioning and operation.
- **Cryptographically secured chain of trust** with all production steps + specific hardware characteristics.
- Use of **Trusted Platform Module (TPM)** and the **Device Identifier Composition Engine (DICE)**.
- **Extend remote attestation** to include hardware characteristics, in addition to software characteristics.
- **Standardize procedures and protocols** within the IETF and Trusted Computing Group (TCG).

## LONG-TERM ANALOG MEASUREMENTS (~1Y)

- Discovery: Temperature and humidity have an effect







## RESULTS

- **Achieved Goals & Results**
  - Identified analog hardware characteristics
  - Long-term measurement of step response in PoCs
  - Verification with remote attestation
  - Standardization success: RFC 9334
- **Planned Results & Current Work**
  - Integration into TPM + DICE ecosystem
  - Standardization in IETF and TCG

Michael Eckel
Fraunhofer SIT | ATHENE Center

WIBU SYSTEMS
Infineon
SIEMENS Ingenuity for life
Fraunhofer SIT
KIT Karlsruher Institut für Technologie
UNIVERSITÄT BIELEFELD
Schölly EXCELLENCE INSIDE
Rev One
RevisionOne Engineering GmbH