

# Confidential and verifiable telemetry using Zero-Knowledge Proofs

Janwillem Swalens, Paarijaat Aditya,  
Lode Hoste, Emad Heydari Beni,  
Majid Salehi

7 May 2026 – zkSummit

The Nokia Bell Labs logo is displayed in white text within a dark blue circular area. The text is arranged in three lines: "NOKIA" on the top line, "BELL" on the middle line, and "LABS" on the bottom line. The "B" in "BELL" is slightly larger and overlaps the "E".

NOKIA  
BELL  
LABS

# Use cases of ZKP

## Payments & Blockchain

e.g. Zcash: shielded transactions,  
zk-Rollup

## Identity & Credentials

e.g. Verifiable Credentials,  
Polygon ID: selective disclosure

## Voting & Governance

e.g. ZKVote,  
DAO governance

## Privacy-preserving analytics

e.g. zkTLS,  
Private set intersection

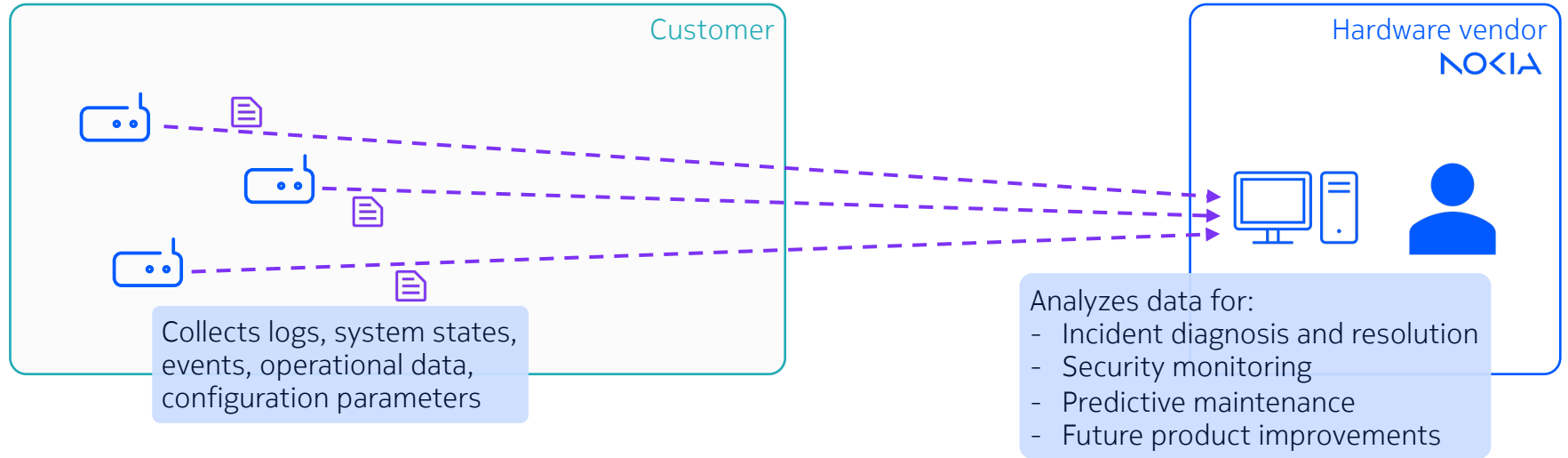
## zkML & Verifiable Compute

e.g. zkML, zkCNN: verifiable ML  
zkVMs: general-purpose computation

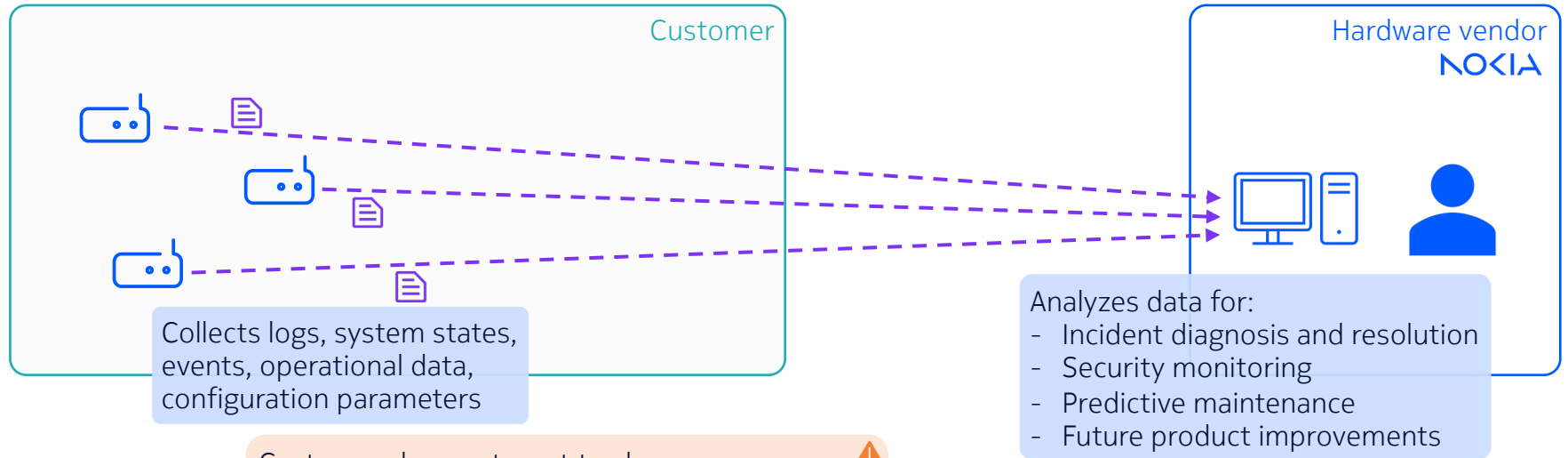
## Telemetry


Our work

# Telemetry set-up



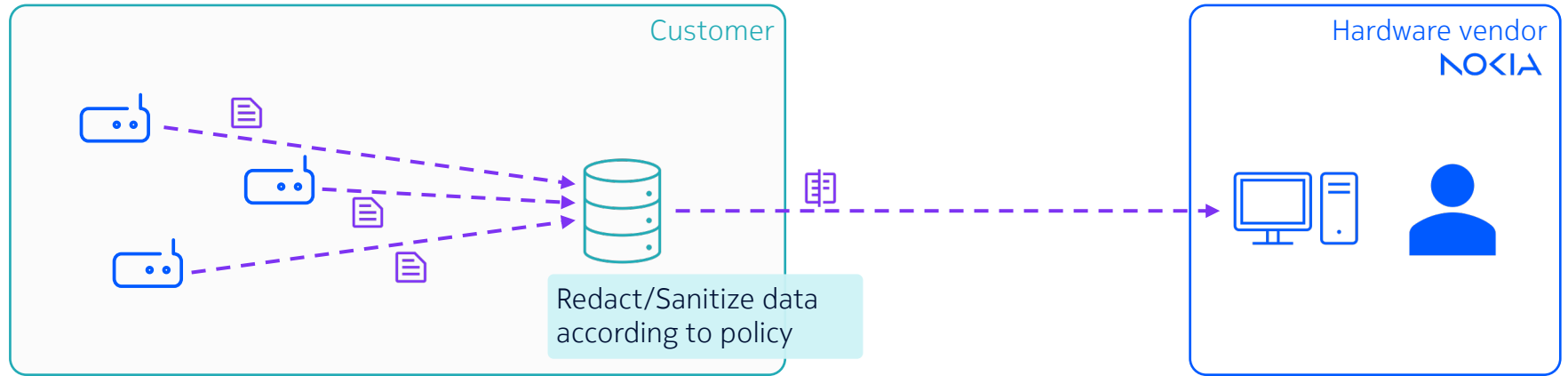
# The customer cares about confidentiality




Customer does not want to share **commercially-sensitive** or **privacy-sensitive** data.   
E.g. IP/MAC addresses, names of systems, information about competitors' devices

Customer may define a **policy** of acceptable data use and transformations.  
E.g. redact IP addresses, only track critical errors

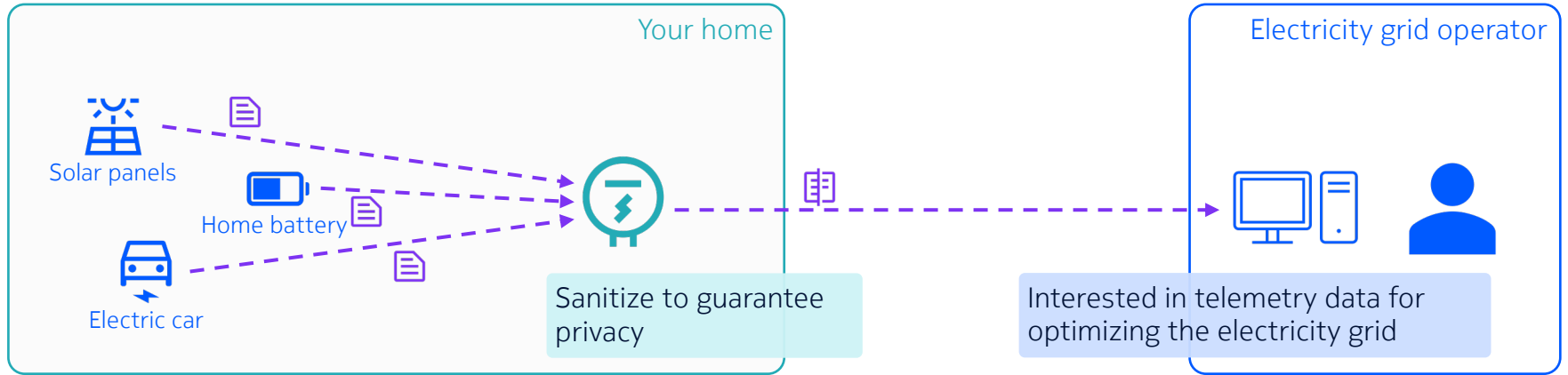
# The vendor cares about authenticity and provenance



How does the vendor know this data  was processed correctly?  
Not doing so may be in the customer's interest!  
The data should be **authentic**.

# Telemetry on end-user devices

E.g. energy management in your home



You do not want to share **private** data.  
E.g. when you are home, which devices you are using



How does the operator know this data was not manipulated?  
This may be in the customer's interest!  
E.g. shift consumption to off-peak hours  
The data should be **authentic**.



# Requirements

## for trustworthy telemetry systems

Vendor manufactures hardware or software that is installed at the customer's premise.

The **customer** desires:



**Confidentiality:** sensitive data must be redacted or sanitized



**Computational integrity:** sanitization must happen according to predefined algorithm (encoding the policy)

The **vendor** desires:

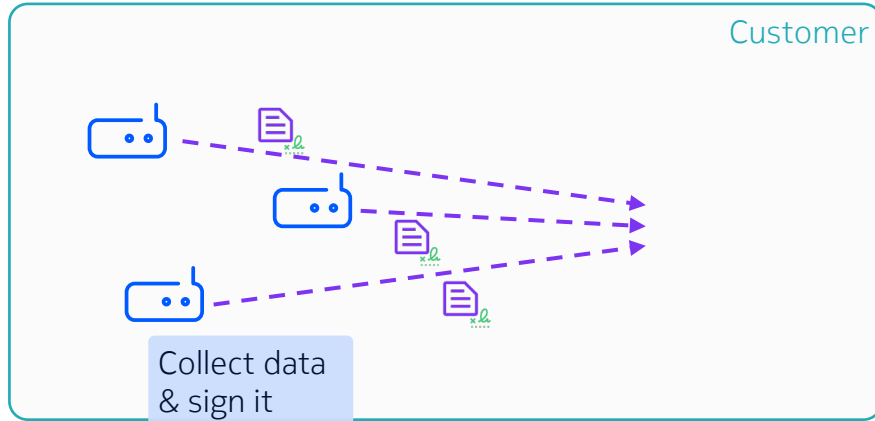


**Authenticity:** original device data was used, no tampering with input

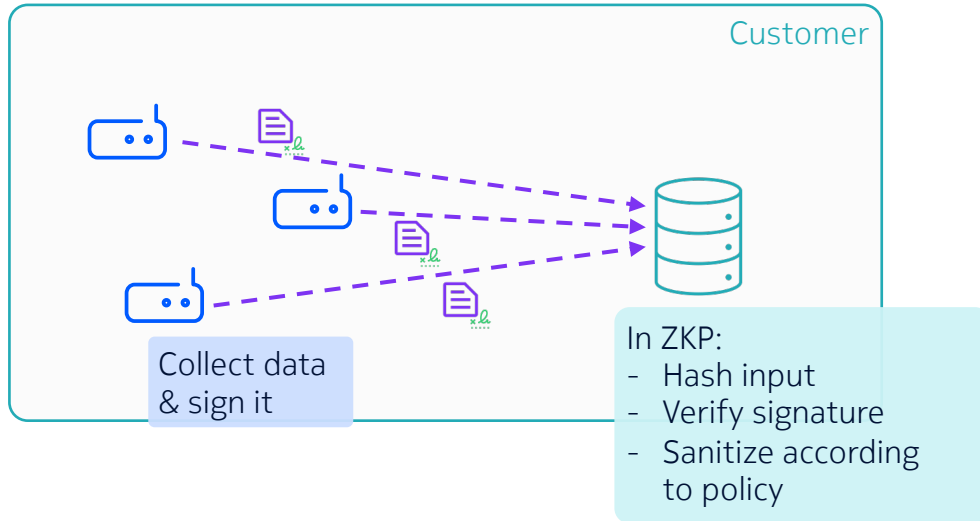


**Computational integrity:** sanitization happened according to agreed-upon algorithm, no tampering with output

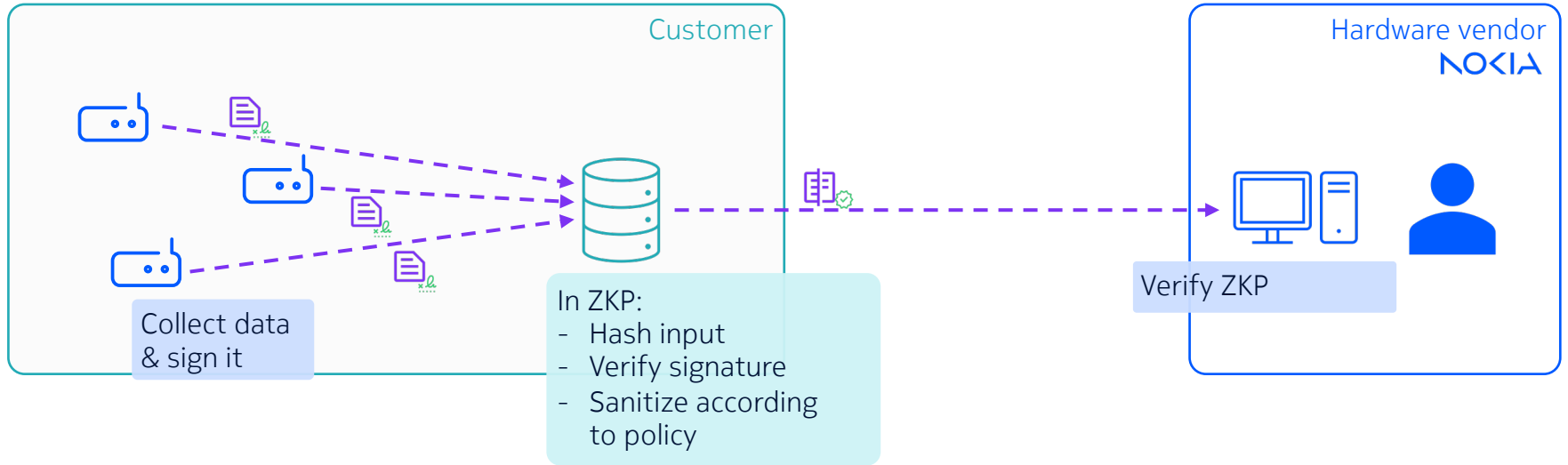
# Protocol: 1. Device signs raw data



## Protocol: 2. Prover redacts data and generates ZKP



# Protocol: 3. Verifier verifies



# This protocol guarantees



## **Confidentiality**

sensitive data is sanitized by customer



## **Computational integrity**

ZKP proves that sanitization happened correctly



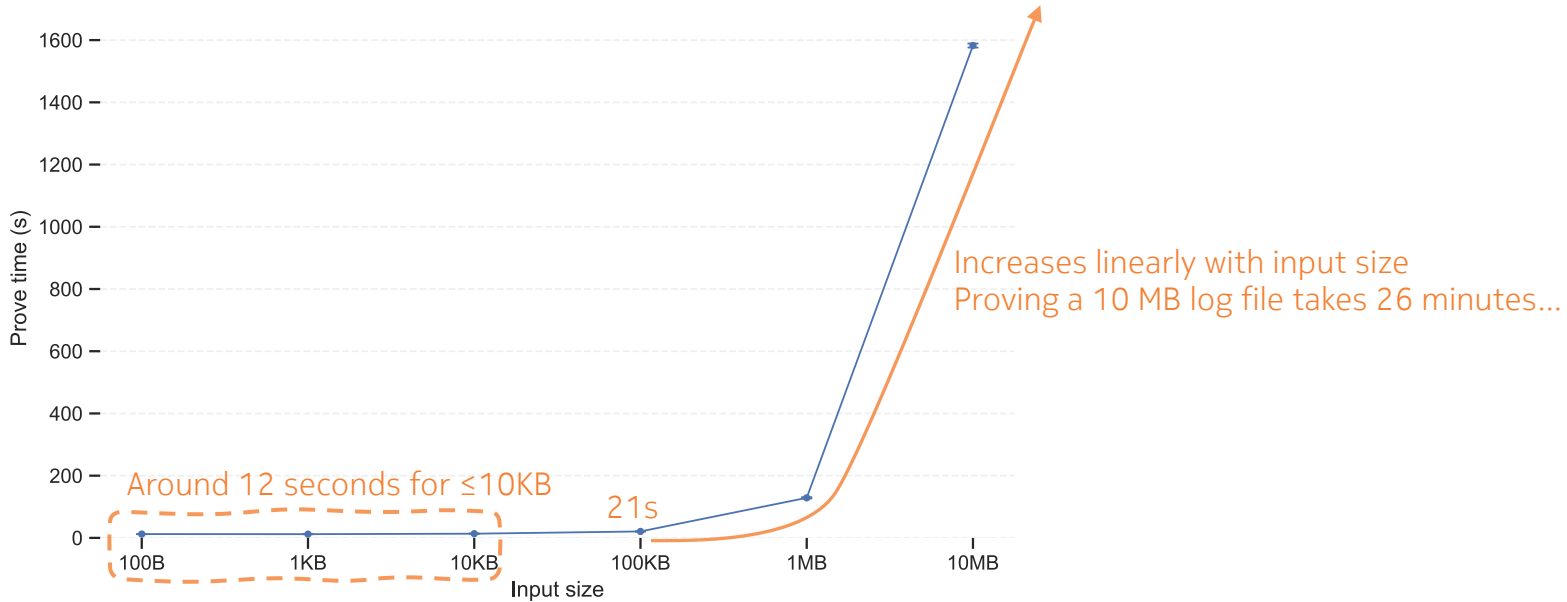
## **Authenticity**

signature proves that original input data was used;  
ZKP proves that output was not manipulated

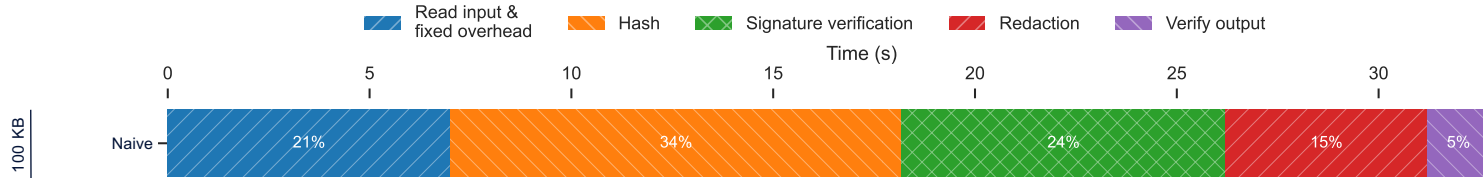
# Performance is a concern for large log files

We deal with large log files!

Some files are over 60 MB: > 1 million lines of logs, command outputs, diagnostics, etc.  
(For resolving incidents, more information is better.)



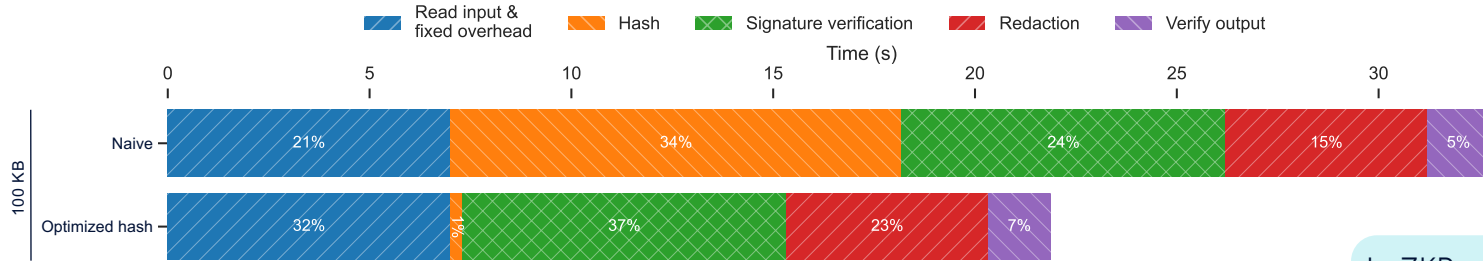
# Performance breakdown



In ZKP:

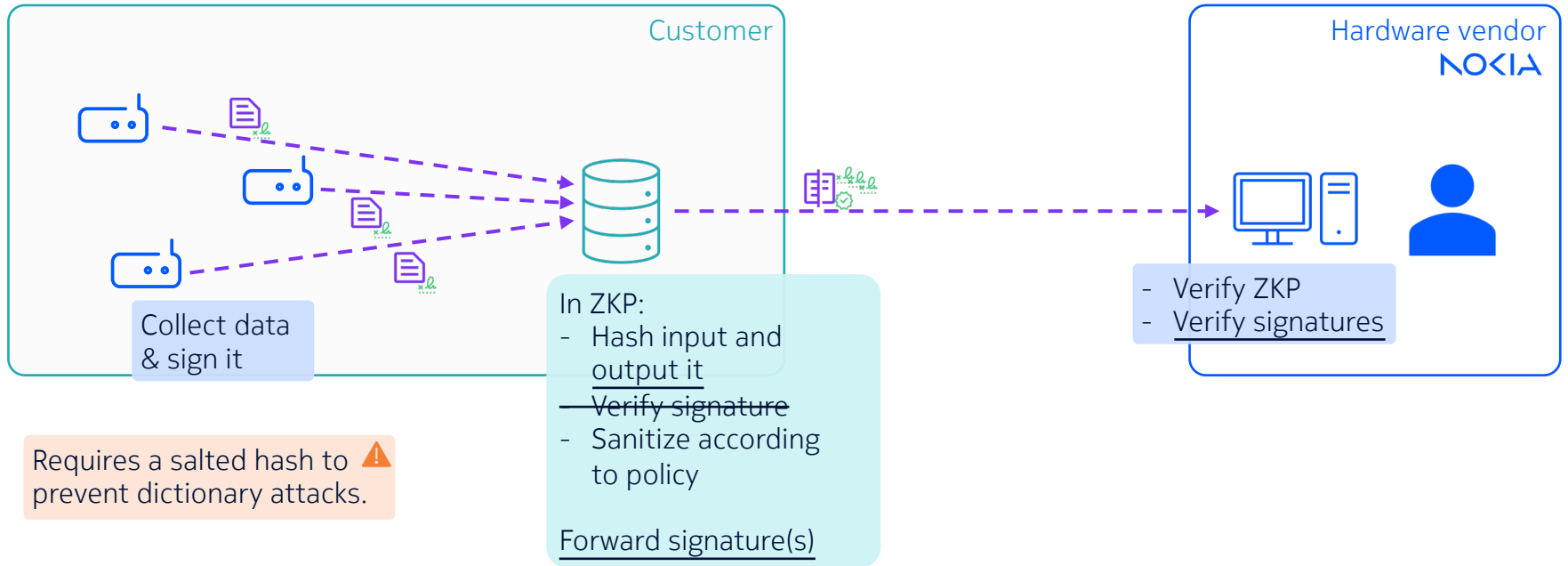
- Read inputs
- Hash input
- Verify signature
- Sanitize according to policy
- Verify if actual output matches expected output

# Performance breakdown

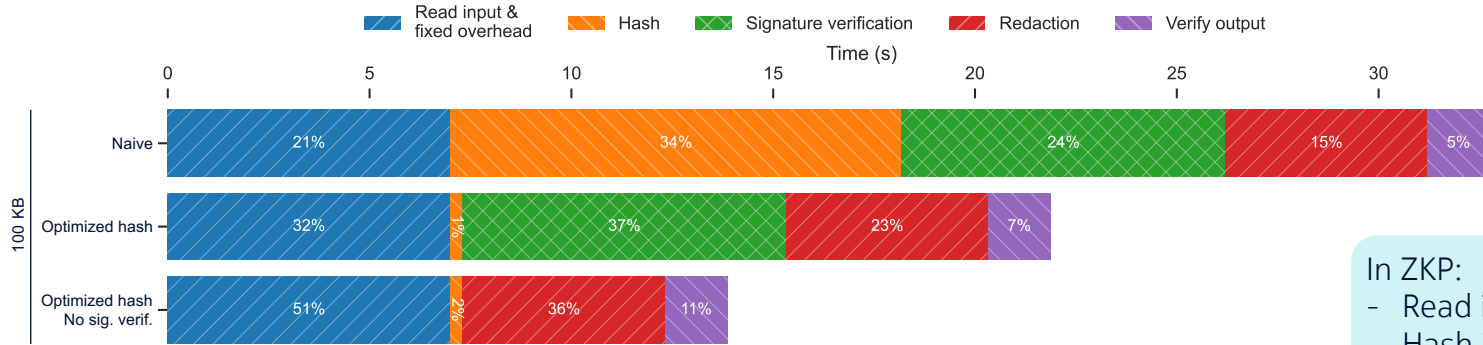


- In ZKP:
- Read inputs
  - Hash input
  - Verify signature
  - Sanitize according to policy
  - Verify if actual output matches expected output

# Outsource signature verification to final verifier

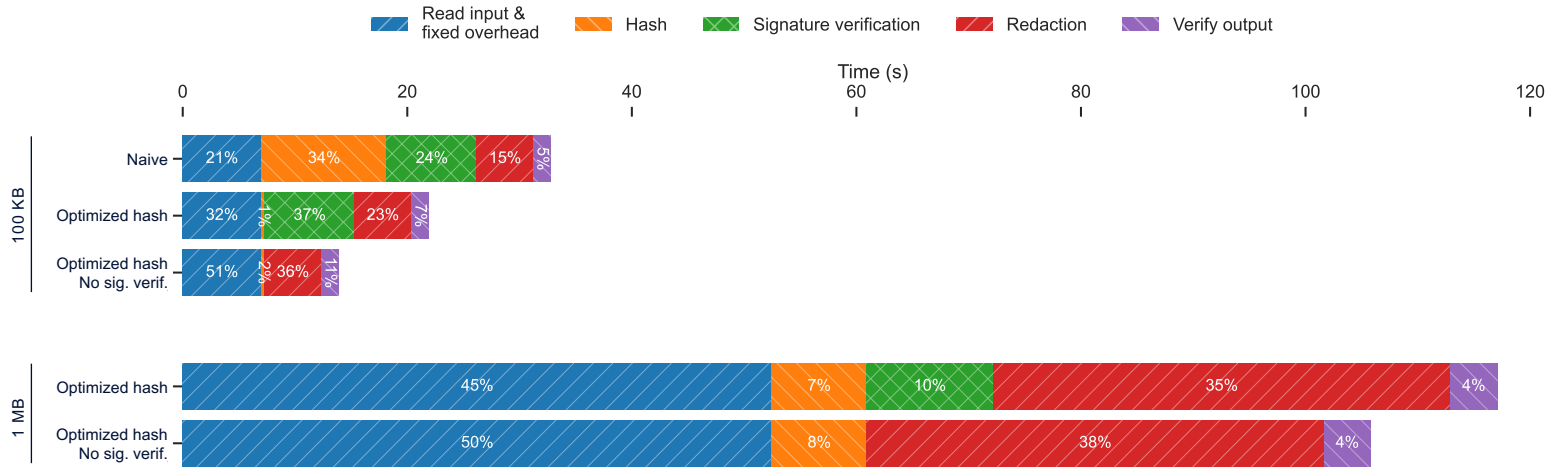


# Performance breakdown

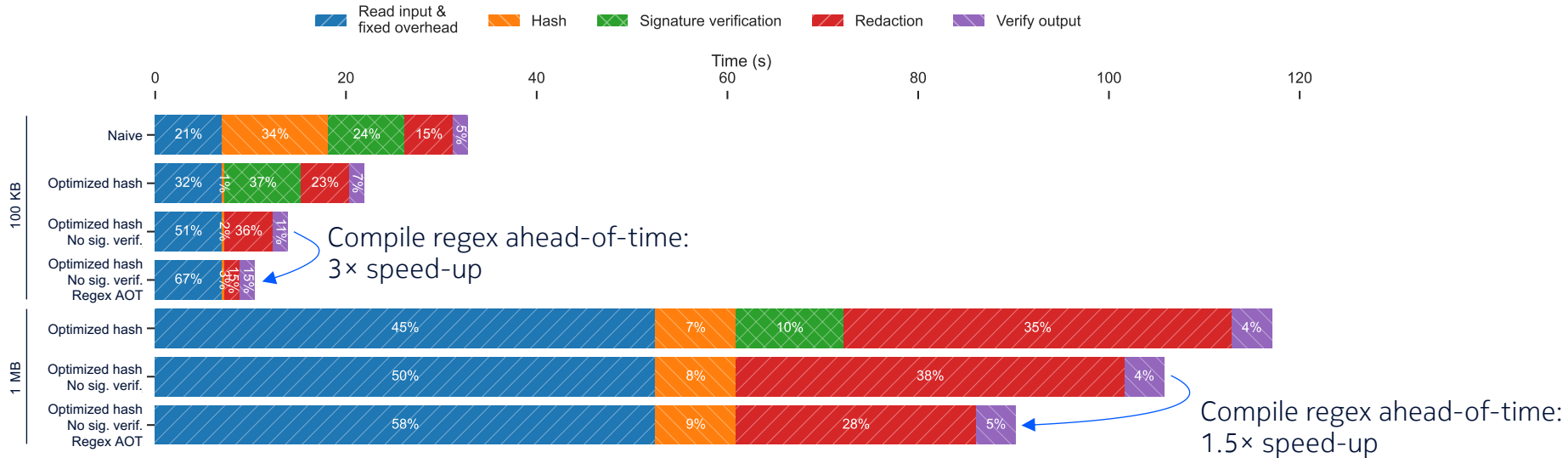


- In ZKP:
- Read inputs
  - Hash input
  - ~~Verify signature~~
  - Sanitize according to policy
  - Verify if actual output matches expected output

# Performance breakdown



# Redaction using regular expressions

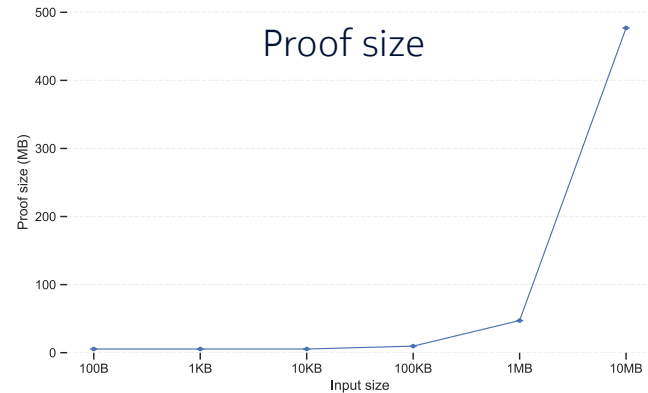
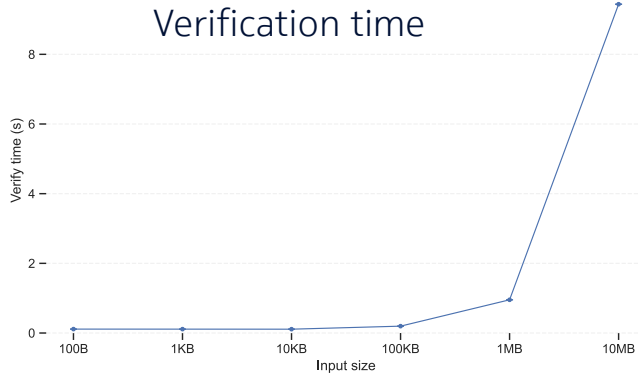
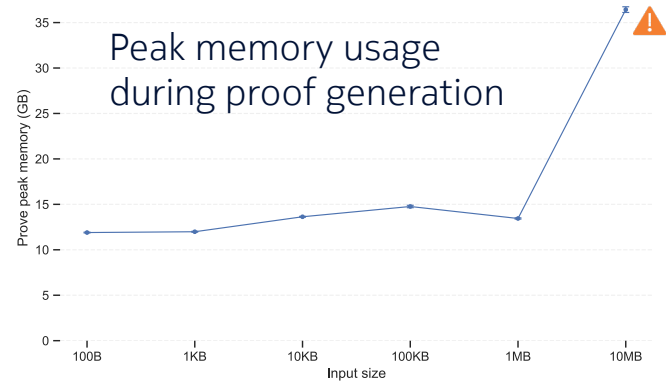
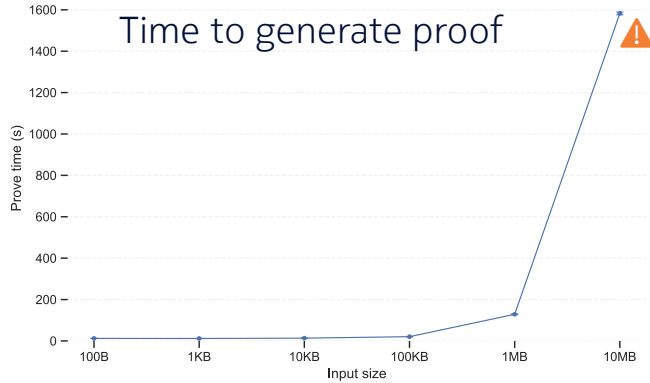


Work in progress: specialized instructions and optimized combination with commitment  
 ⇒ ~15× speed-up compared to original

Related work:

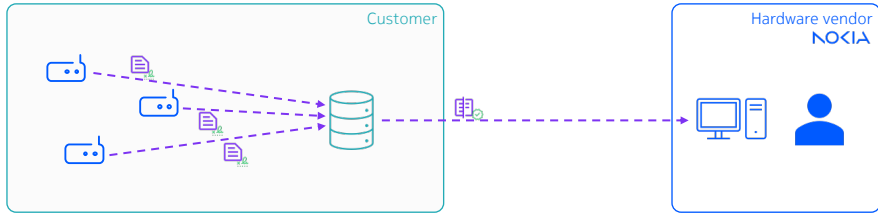
- Raymond et al. (2023). “Efficient zero knowledge for regular language.” In *International Conference on Security and Privacy in Communication Systems*.
- Luo et al. (2023). “Privacy-preserving regular expression matching using nondeterministic finite automata.” In *Cryptology ePrint Archive*.
- <https://github.com/zkemail/zk-regex>

# What about: memory usage, verification time, proof size?

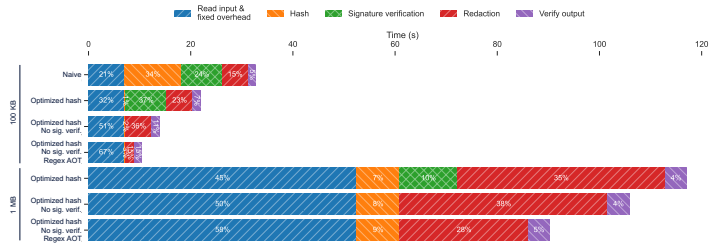


# Summary & open challenges

We have been exploring a novel use of ZKPs for **verifiable and confidential telemetry**, guaranteeing **confidentiality** of sensitive data for the customer, **authenticity** of the data to the hardware vendor, and **computational integrity** of the predefined sanitization algorithm.



This has required many tricks and optimizations to **improve performance**, and will require even more **for large inputs**.



- Hashing, commitment to input
- Signature verification
- Parsing data
- Regular expressions
- Encryption/Decryption

Other challenges:

- Long-term support (decades!)
- Standardization?

NOKIA  
BELL  
LABS

# Copyright and confidentiality

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use by Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback").

Such Feedback may be used in Nokia products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular

purpose, are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.