Security of xApps – Concept for automated permissions checks

Berlin Open RAN Working Week

Heiner Grottendieck | Head of Division Security for 5G/6G Infrastructure at BSI

10 September 2025

Federal Office
for Information Security

Brief profile of BSI – Federal Office for Information Security

Foundation
1 January 1991

238 million euros budget 2024

Posts in 2024

1.785

BSI presence

Sites

Offices

Liaison offices

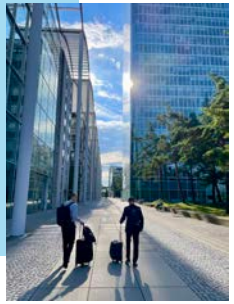
Furthermore, the BSI has long been playing a key role on international levels, including close cooperation with bilateral partners and multilateral fields of action relating to EU and NATO.

BSI 5G/6G Competence Center

The 5G/6G Competence Center in Freital is tasked with coordinating all BSI measures aimed at strengthening cybersecurity, resilience and the sovereignty of Germany and EU in the field of 5G/6G.

Public Mobile Networks

- Product Certification of critical components
- MNO Auditing
- Catalogue of security requirements for public MNOs (Security Catalogue) (with BNetzA)



Private Mobile Networks

- Security guidelines to ensure baseline protection and resilience

5G/6G Security Lab „TEMIS“

- Evaluation & testing of security solutions
- Technical collaboration with industry and academic partners

Risk Analysis

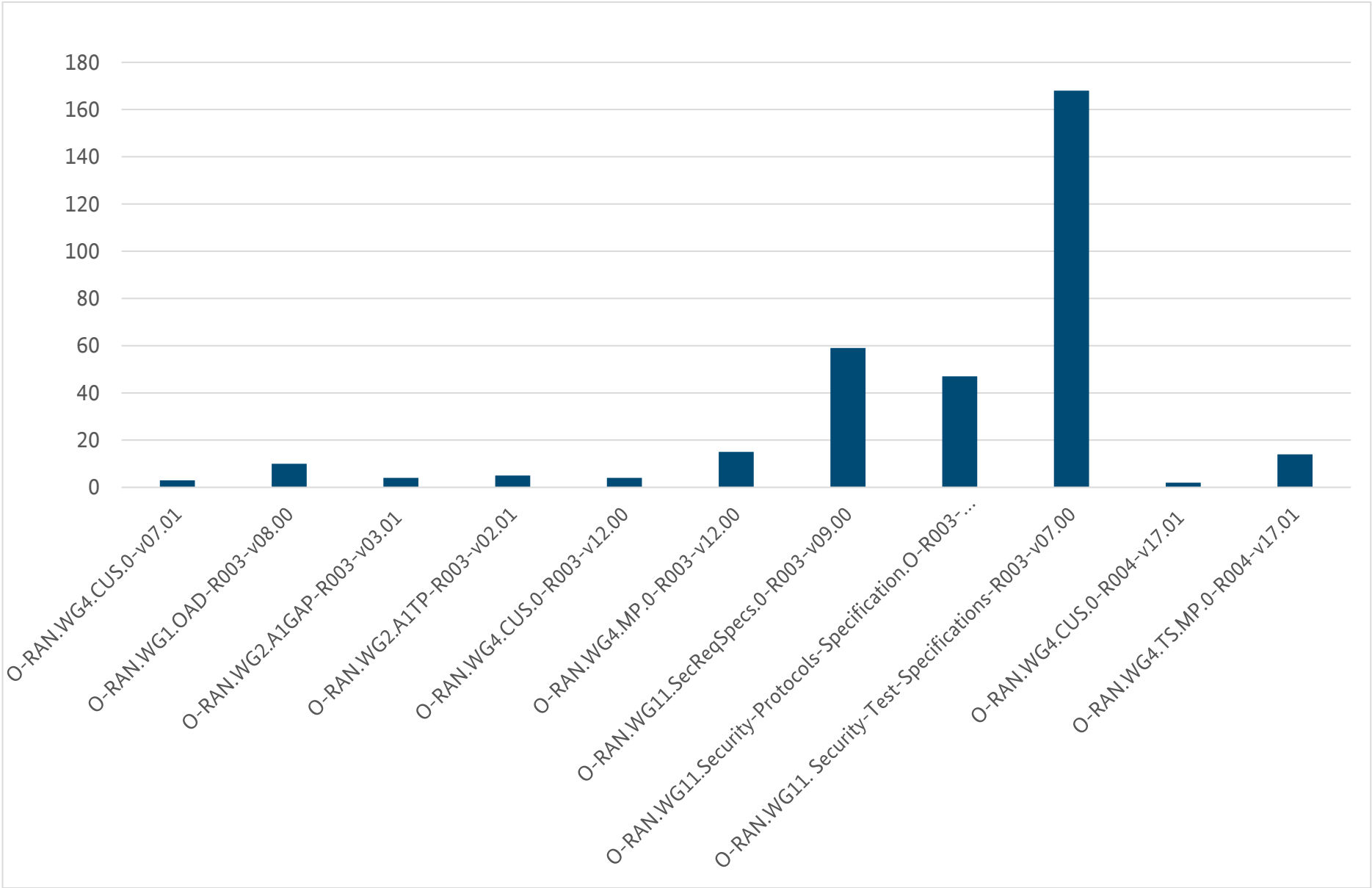
- Open RAN Risk Analysis
- Comprehensive 5G Risk Analysis

Standardisation

- Contributions to 3GPP, GSMA and ETSI
- Engagement in EU regulatory initiatives

enisa European Network and Information Security Agency
ETSI
GSMA
3GPP A GLOBAL INITIATIVE

Number of BSI comments in ETSI MSG PAS process



Open RAN – Still Not Secure by Design?

Insights from recent years in ETSI MSG

Good progress in O-RAN documents regarding security

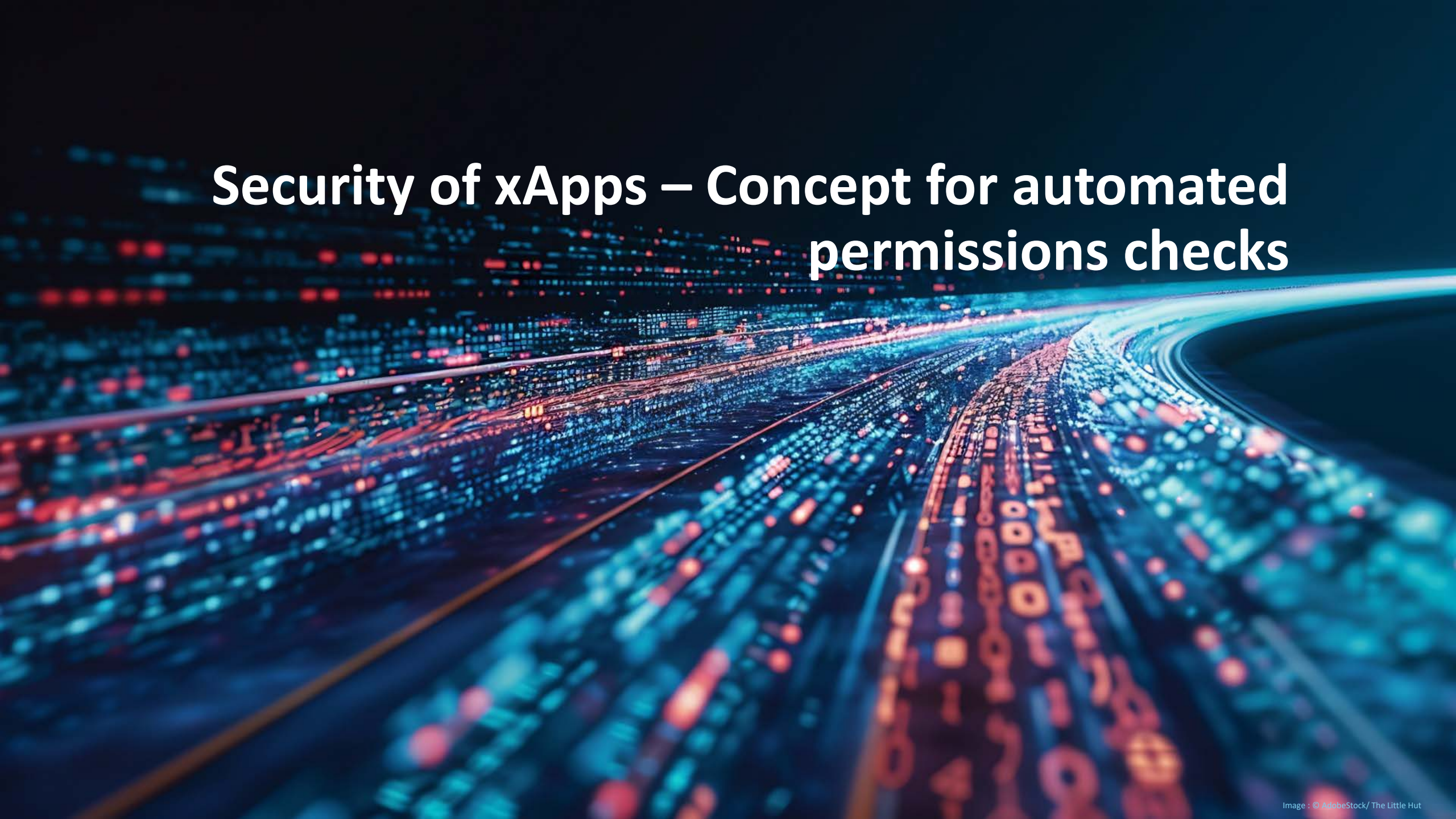
- Working Group 11 with benefits for O-RAN Security
- O-RAN specific security tests – important milestone
- 4 fundamental O-RAN Security Documents passed ETSI in 2025

But still…

- O-RAN specifications not yet fully consistent regarding security
- Security tests – mapping tests vs. components needed
- Backwards Compatibility (e.g. Open Fronthaul) inhibits Security partially
- Commitments made by the Rapporteurs in ETSI do not seem to be binding

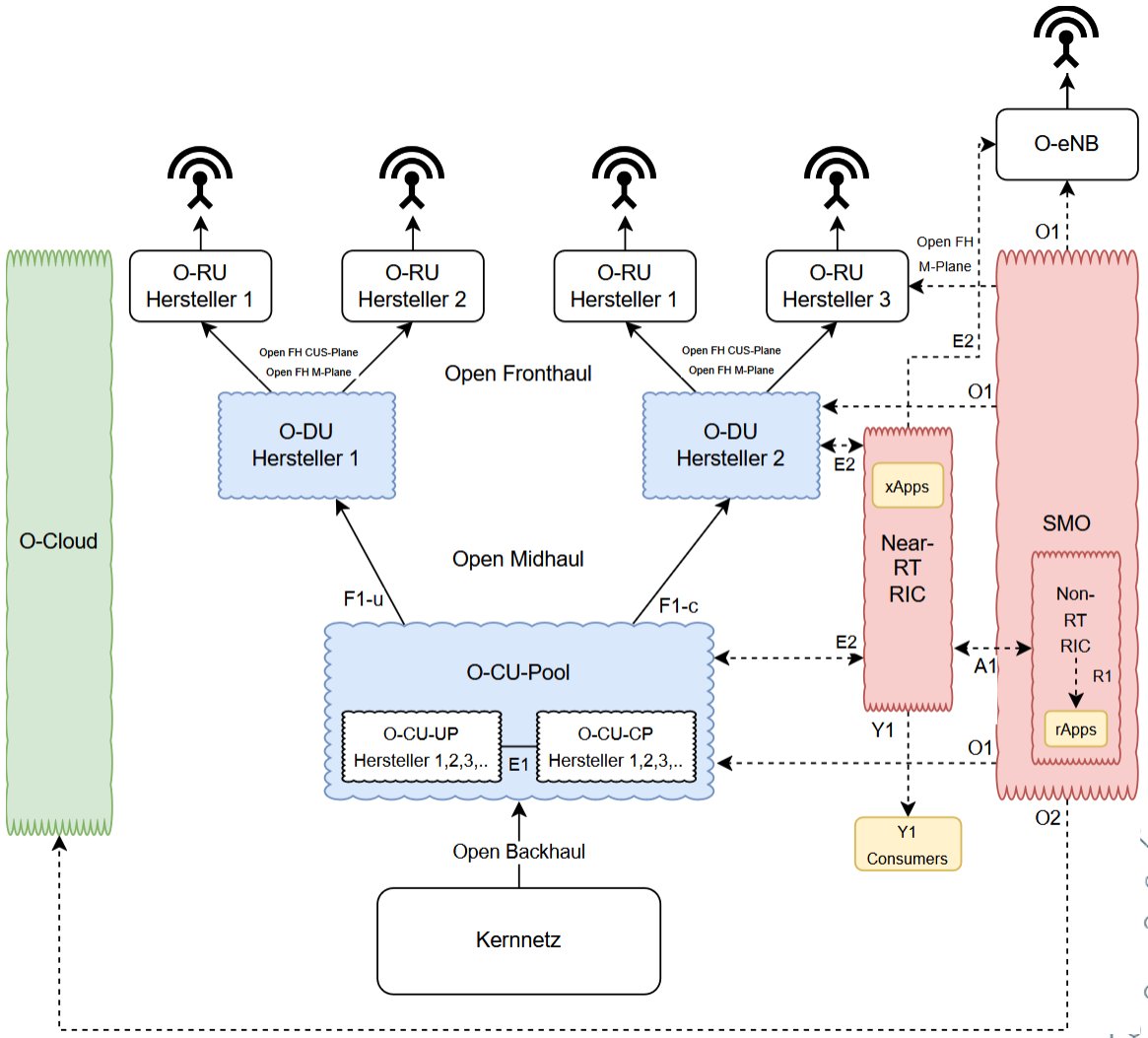
➢ Still room for improvement

Security of xApps – Concept for automated permissions checks



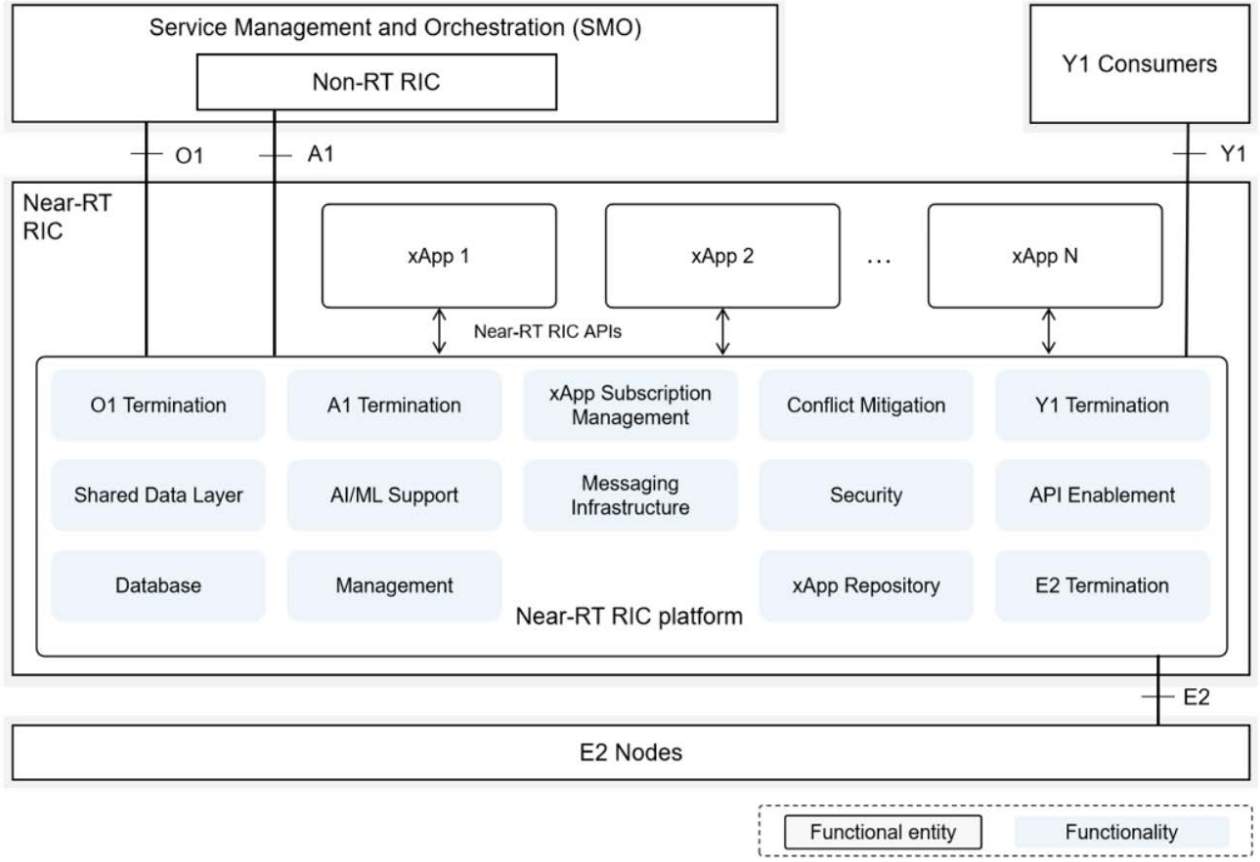
xApps

- Microservices for intelligent network optimization
- Can be provided by third-party vendors
- Possibility to quickly add functions to the network
- Examples: Traffic steering, Handover optimization, Energy optimization



Execution environment for xApps – Near RT RIC

- Near-RT-RIC provides execution environment for xApps
- xApps receive data via Shared Data Layer
- Near-RT-RIC connects xApps with network components (“E2 nodes”)



Source: O-RAN Alliance

Onboarding of xApps

- Usually deployed as containers
- Registration with Near-RT-RIC
- Registration request contains configuration file with ports, requested permissions, functions, and messages
- **Requested permissions are granted without further verification**

xApps: the central problem

- permissions are granted without verification
- Possible violation of the Principle of Least Privilege
- Risks in case of a compromised xApp:
  - Manipulation of network parameters
  - Data leakage
  - Service quality impairment
  - Creation of movement patterns
  - …

Objective for xApps Security

- **Automated evaluation of task adequacy** of permissions requested by xApps
- Security gain for O-RAN without restricting flexibility

Concept & Approach

Image : © AdobeStock/Azazul

Integration into Architecture

- Implementation in Near-RT RIC
- Architecture has placeholder component “Security”
- Provides AI/ML support for intent-based approaches
- Local execution is mandatory due to security relevance
- Configuration file already provided

→ **No change in permissions assignment processes / architecture necessary**

- Only additional step in the onboarding process
- Choice of an intent-based approach

Automated permissions evaluation

- Use of AI to assess whether permissions match the intent
- Primary use of Large Language Models (LLMs)
  - Context understanding
  - Natural language comprehension
  - Provide explainable decisions
- Other ML models can perform similarity checks/classification, but cannot provide reasoning
- Important: Local installation of the ML model!

Role of the administrator

- Due to security relevance, final decision should be made by the administrator
- Preparation of permissions + mapping + evaluation by LLM for minimal human workload
- Optionally fully automatable (e.g. in CI/CD pipelines)
  - In case of suspicion: stop onboarding + notify administrator

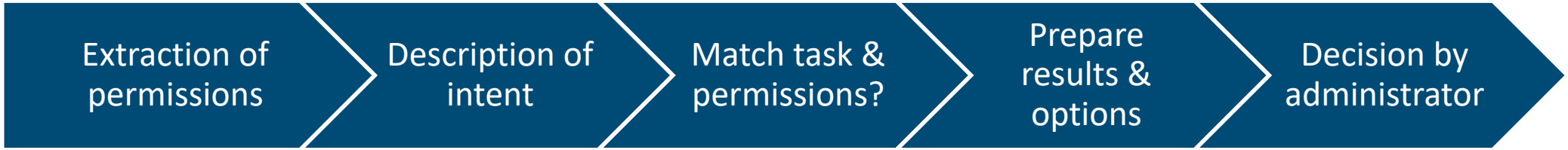
Verification times

- When onboarding a new xApp
- During update or downgrade
- With configuration changes
- At regular intervals (e.g. daily)

→ All use the same configuration file = no distinction necessary

→ Regular verification at all relevant lifecycle stages for continuous security

Concept - overview



- JSON file from onboarding
- Parsing or ML based

- text file from onboarding

- Computed by LLM
- Prompt engineering usable

- Command line output
- Show mapping permissions → tasks
- Evaluation of permissions + reasons

- Final decision by human
- Continue or cancel installation

Proof of Concept

Proof of Concept

- Demonstration of technical feasibility of the concept
- Evaluation of accuracy and practicability
- Testing with realistic scenarios using original demo xApps
- Comparison of several AI models

Selection of LLMs

- Deepseek R1:
  - strong media presence, very powerful, commercially freely available locally
- Mistral Large:
  - largest LLM developed in Europe
- Qwen2.5:7b_q6k:
  - Local Kubernetes cluster with Ollama + RTX 3070
  - Chosen model: Qwen2.5 due to explicit training focus on JSON evaluation

Test data

- 7 original demo xApps from O-RAN SC, unchanged
- Manipulated demo xApps with added permissions
  - 2 test groups: “obvious” manipulated + “harder to detect”
- Manipulated demo xApps with added permissions and modified intent
- Intent = introductory paragraph of Github / Wiki project documentation
  - Example: “This is a Traffic Steering xApp. It consumes A1 Policy Intent, listens for badly performing UEs from Anomaly Detection xApp, sends prediction requests to QP (Quality Prediction) xApp, and listens for messages from QP that show UE throughput predictions in different cells to make decisions about UE Handover.”
- Total: 28 test cases, each conducted 100x = 2800 API calls per LLM

Evaluation by LLM

- 4 evaluation categories per permission:
  - Necessary
  - Unnecessary
  - Necessary + Check recommended
  - Deprecated
- Example output:

Requested Right/Function	Necessity	tx/rx	Port-Number	Explanation of Right/Function	Mapped Task + Relevance
RIC_SUB_REQ	Necessary	tx	4560	Initiates subscription to receive specific data from network components.	Required to set up subscriptions for performance testing, enabling the xApp to request data from the RIC.
RIC_SUB_DEL_REQ	Necessary	tx	4560	Requests deletion of existing subscriptions.	Needed to clean up subscriptions after testing, ensuring proper resource management.
RIC_SUB_RESP	Necessary	rx	4560	Confirms subscription request success/failure.	Essential to validate subscription setup, ensuring the xApp receives the expected data for analysis.
RIC_INDICATION	Necessary	rx	4560	Carries actual performance/event data from network components.	Core to the task: Receives real-time data for benchmarking and analyzing RIC/platform behavior.
RIC_SUB_DEL_RESP	Necessary	rx	4560	Confirms subscription deletion success/failure.	Ensures proper cleanup of subscriptions, aligning with infrastructure testing lifecycle management.

The rights are appropriate.
All requested rights directly support the xApp's task of performance benchmarking, including subscription management and data collection. No unnecessary or deprecated rights are present. Each right aligns with the described intent to test infrastructure and observe system responses.

Results

PoC Results in figures

ML-Modell	False-Positive-Quote	Detektionsquote manipulierter xApps		Korrekte Klassifikationsquote aller xApps	
		exkl. Check	inkl. Check	exkl. Check	inkl. Check
Deepseek R1	0,17 %	62,52 %	81,90 %	71,79 %	86,39 %
Mistral Large	0,17 %	43,90 %	50,43 %	57,14 %	62,79 %
Qwen2.5:7b_q6	1,5 %	13,57 %	28,38 %	32,14 %	45,35 %

Findings

- LLMs with larger models deliver significantly better results
- False-positive rate <0.2% achievable → good practical applicability
- Even with smaller models theoretically possible, but only limited usefulness
- Up to 81.9% detection rate = very good result for a proof of concept

Conclusion

- O-RAN xApps & permissions assignment thoroughly analyzed and solution approaches identified
- Concept developed & possibilities outlined
- With the proof of concept, practical feasibility was demonstrated
- Encouraging PoC results – with room for improvement
- **What about your O-RAN deployment?**

Credits to the author

- Master Thesis of Eric Sabitzer at BSI:

  Sicherheit von xApps in Open RAN: Konzept zur automatisierten Rechtebewertung. – 2025. – 87 S. Mittweida, Hochschule Mittweida – University of Applied Sciences, Fakultät Angewandte Computer und Biowissenschaften, Masterarbeit, 2025.

- Prof. Dirk Pawlaszczyk, Hochschule Mittweida
- Dr.-Ing. Stefan Köpsell, Barkhausen Institut
- More Details?

  Please, contact BSI / S 31

HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

barkhausen institut

Thank you for your attention!

Heiner Grottendieck
Head of Division Security for 5G/6G Infrastructure (S 31)
heiner.grottendieck@bsi.bund.de

Federal Office for Information Security (BSI)
Godesberger Allee 87, 53175 Bonn

Visit us at Hüttenstraße 14, 01705 Freital

www.bsi.bund.de

Federal Office
for Information Security

Follow us: