RADIX SECURITY
www.radix-security.com

Challenges and Solutions in 5G Certification

A German Perspective

David Rupprecht - 19.01.2024 - fuse5G - Utrecht, NL

101 Weeks

Until Germany Operators are only allowed to deploy certified 5G equipment.

Agenda

101 Weeks

Challenges:

German 5G Certification (NESAS-CSS-GI)

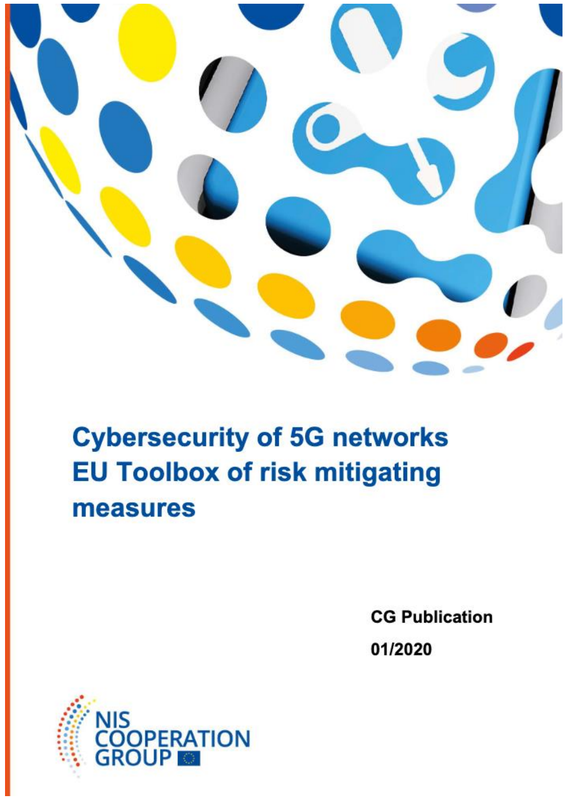
Improvement:

5G Certification

EU 5G Toolbox

Actions to enhance 5G security at European level

- In 2020, the EU 5G Toolbox was published, which defines the risks of the 5G network and how to increase its security.
- Just a recommendation for member states
- No mandatory 5G certification on a European level yet.
- Example: TM02: Ensuring and evaluating the **implementation** security measures in existing 5G standards



Germany: 5G Certification

- Motivation:
  - Increase the security of mobile communication
  - Encounter a ban on certain vendors
- Different laws cover different aspects (TKG, BSIG)
- Important players:
  - BSI (Federal Office for Information Security)
  - BNetzA (Federal Network Agency)

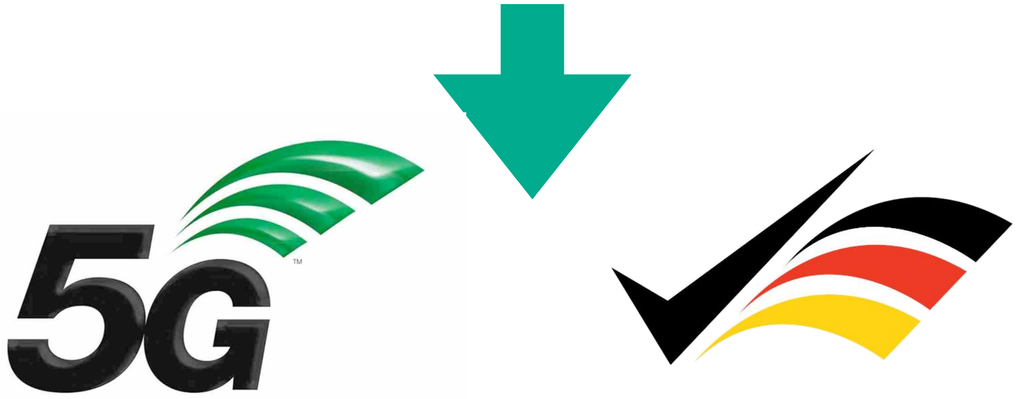
Network products deployed by 2026 in 5G networks must be certified

Certification scheme requirements

- Reproducibility
- Verifiability
- Independence
- Security Level (CSA):
  - Low
  - Medium
  - High
- Market Adoption

Possible 5G certification schemes

- Common Criteria (CC)
- Beschleunigte Sicherheit Zertifizierung
- **NESAS-CCS-GI**



BSI NESAS-CCS-GI

Network Equipment Security Assurance Scheme

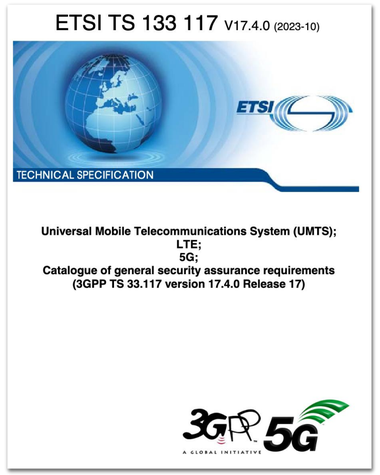
- Based on the GSMA NESAS Scheme
- **Review of the security development lifecycle:**
  - The auditor checks the security development life cycle at the vendor
- **Product Evaluation:**
  - Evaluation facility applies security test
  - **3GPP SCAS test cases** are the base for the certification

3GPP SCAS

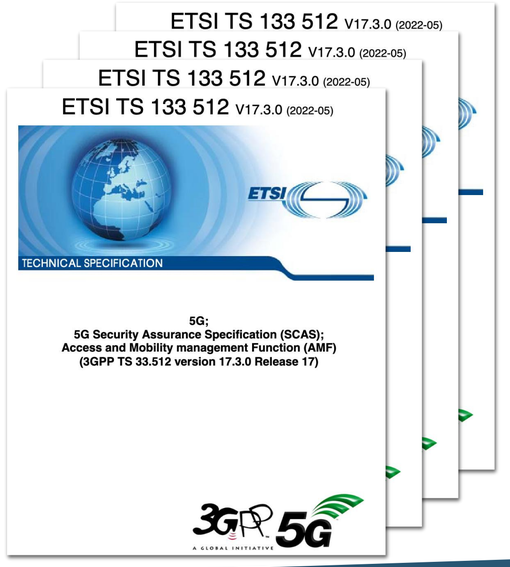
Security Assurance Specification

- SCAS: Security Assurance Specification
- Defined by the 3GPP (3rd Generation Partnership Project)

General Test Cases (33.117)



Specific Test Cases (33.5XX)



Challenges of NESAS-CCS-GI

NESAS-CCS-GI

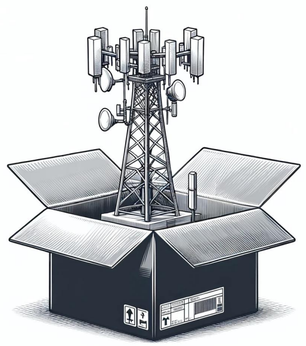
Certification in a Nutshell

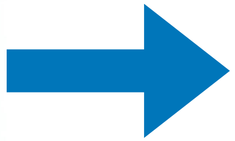
Vendor

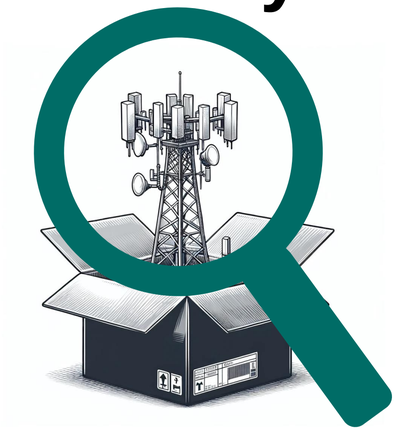
Evaluation Facility

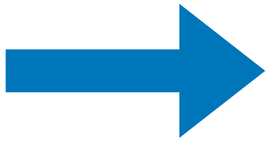
Bundesamt
für Sicherheit in der
Informationstechnik

Operator







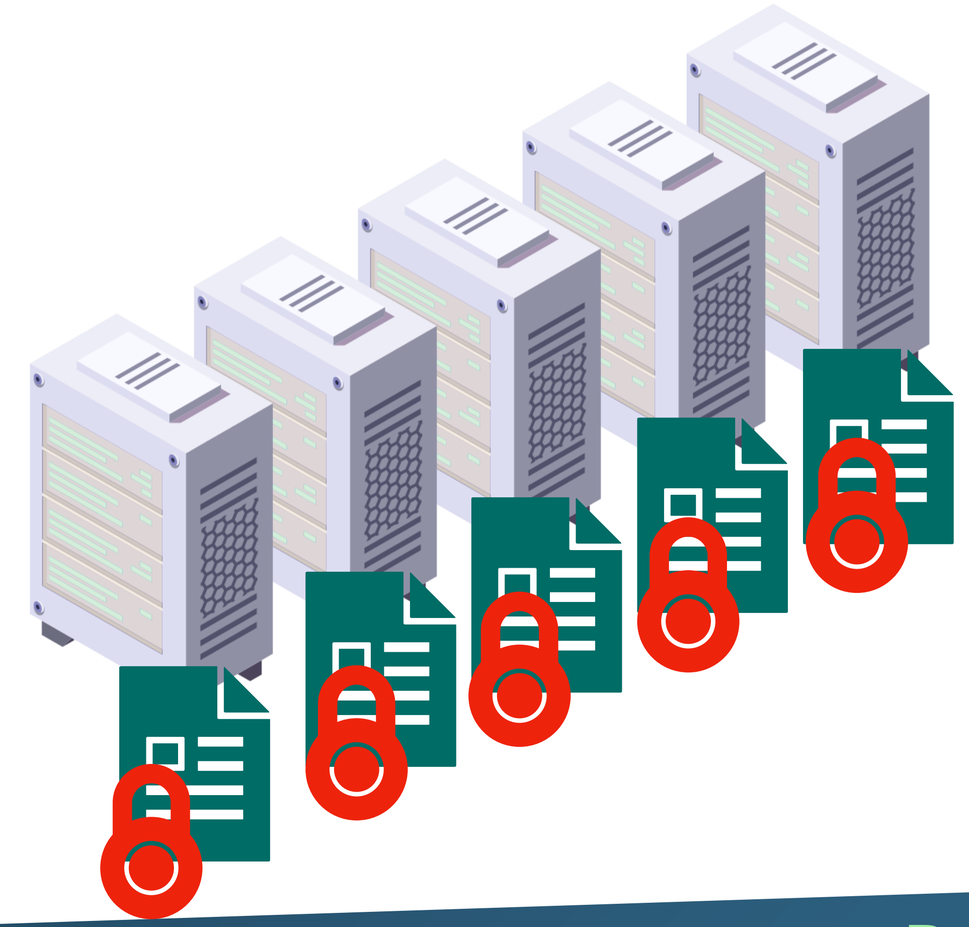


Time to certify a network component

- Linear approach to certification
- Certification can take up to a few months
- Equipment is shipped to an evaluation facility
  - Needs to be configured at the evaluation facility
- Vendors have up two releases in a quarter
- Might hinder a wide market adoption

Deployment Security (Configuration)

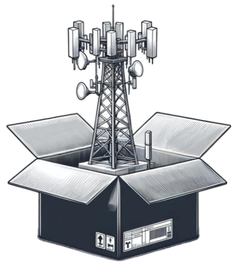
- The scheme focuses on the implementation of security
- The deployment (configuration) is not considered
- The configuration can impact the security



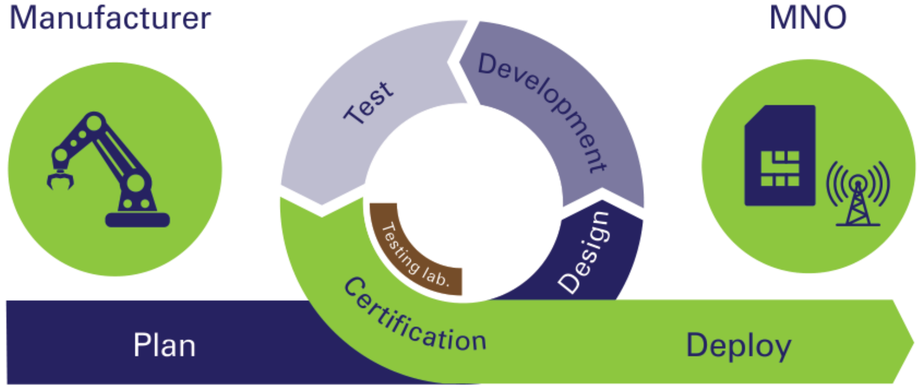
Improvements for NESAS-CCS-GI

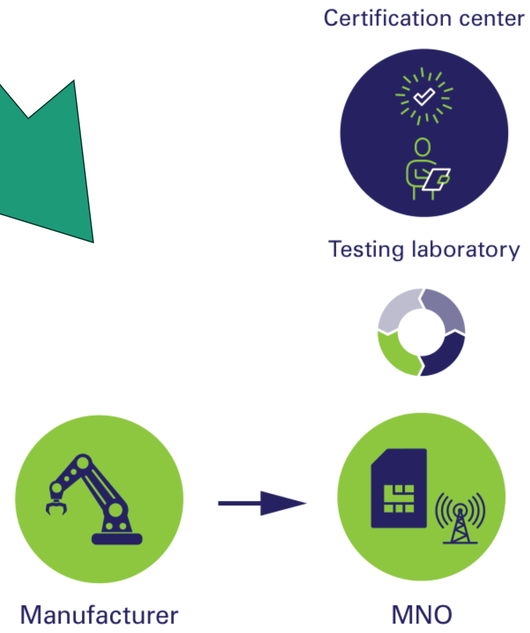
Improvement of 5G Certification

Left Shift



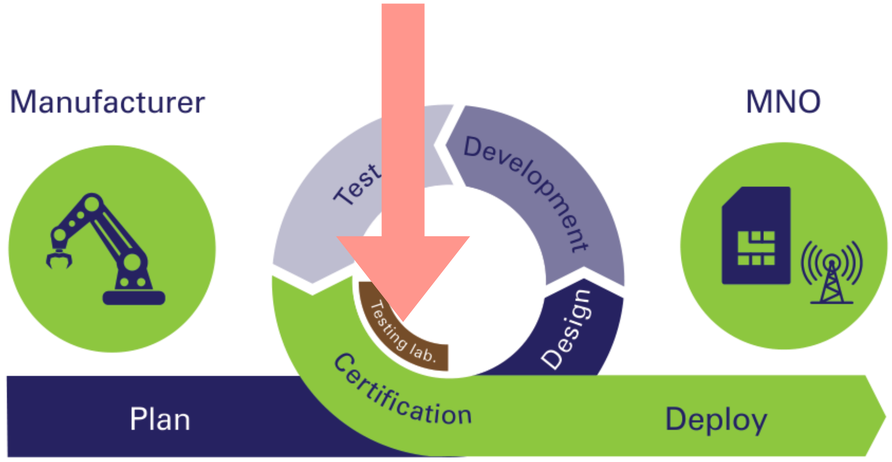
Right Shift





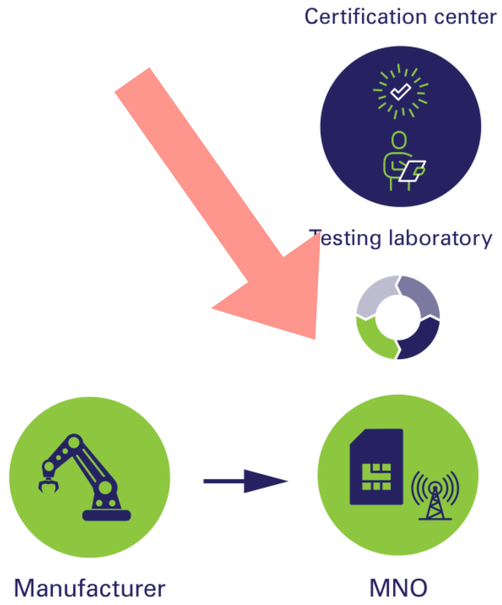
Certification Approach - Left Shift

- Idea:
  - Integrating the certification into the existing Development/Testing cycle
- Advantages:
  - This decreases the setup time and testing at the test lab
  - Overall it reduces the cost of certification time
- Challenges:
  - The testing lab needs to be independent
  - The overall issue of security of deployment is left open
  - **Test cases must be automatable**



Certification Approach - Right Shift

- Idea:
  - Moving the certification to the operational/live network environment of the MNO.
- Advantages:
  - This decreases the overall setup time.
  - Addresses the configuration and deployment
- Challenges:
  - Test cases may require non-standardized 3GPP behavior
  - **Test cases must be automatable**



Automating SCAS Test Cases

- **Automatable**
  - The tester sends XYZ to the device under test and expects ABC as a response.
- **Automatable with vendors' cooperation**
  - The tester logs in on the console, adds a user with a specific role, and verifies that the user has the correct permissions.
- **Non-automatable**
  - The tester reviews the documentation
- Not all are applicable => virtualized network product, no USB stick test

SCAS Test Automatisation

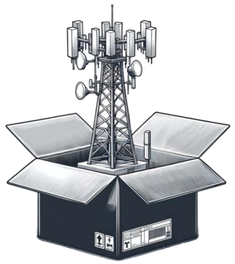
Challenges and Solutions

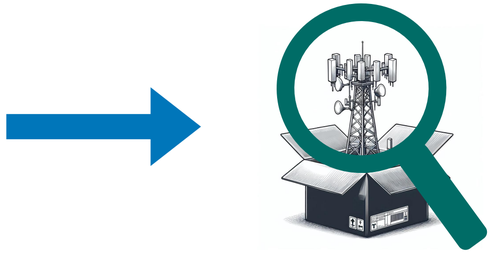
- For the 81 General SCAS (33.117) test cases, we see:
  - 21 are automatable — straightforward to handle
  - 49 automatable but requires vendor cooperation
  - 11 aren't automatable
- For the 16 AMF test cases, we can automate:
  - 15 of them
  - 1 requires vendor cooperation
- For both the UDM and NRF, all the test cases are automatable.

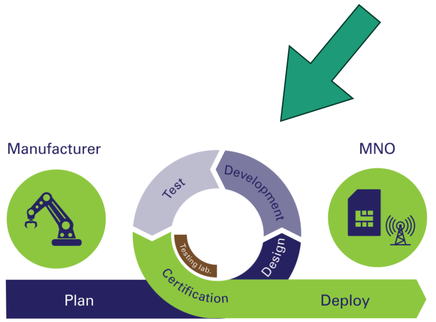
~80%

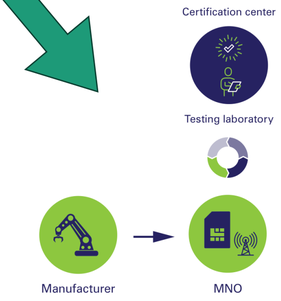
Conclusion

101
Weeks









Thanks you & Questions