5G Security

(And Why You Should Care About It)

Montsecure

About Us

David Rupprecht

- Expert on 4G and 5G Security
- 9+ years researcher at Ruhr University Bochum
- Founder & CEO of Montsecure

Christoph Heine

- Experienced in REST Security
- Specialized in automation of pentesting frameworks
- Project Manager & Developer at Montsecure

About Us

David Rupprecht

- Expert on 4G and 5G Security
- 9+ years researcher at Ruhr University Bochum
- Founder & CEO of Montsecure

Christoph Heine

- Experienced in REST Security
- Specialized in automation of pentesting frameworks
- Project Manager & Developer at Montsecure

5G Pentesting Tools

Introduction to 5G

5G Basics

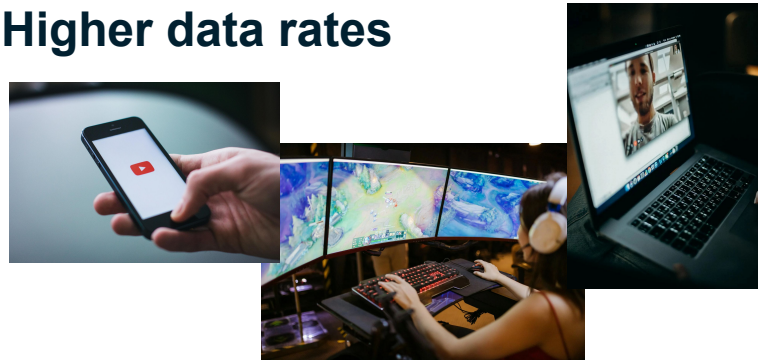
- **5G == 5**th **G**eneration standards for mobile network
  - Specified by 3GPP standards organization
  - Evolved from previous standards: 4G (LTE), 3G (UMTS), 2G (GSM), …
- Developed since 2008
- Introduced in 2016
- Rolled out in practice since 2019
- Adoption in phone networks worldwide by 2025: ~25% of connections

Goals of 5G Standards

Higher data rates	Massive Internet of Things
Ultra Reliable & Low Latency	Small Scale & Modular Networks

Goals of 5G Standards

Higher data rates



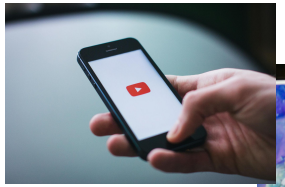
Massive Internet of Things

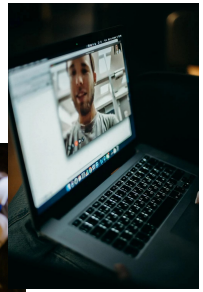
Ultra Reliable & Low Latency

Small Scale & Modular Networks

Goals of 5G Standards

Higher data rates





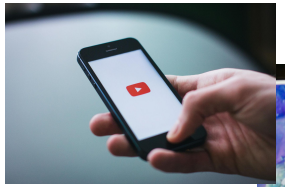
Massive Internet of Things

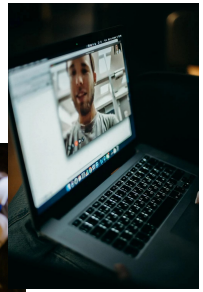
Ultra Reliable & Low Latency

Small Scale & Modular Networks

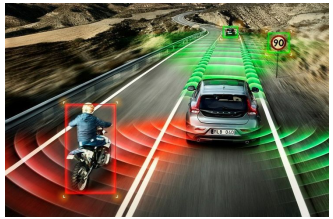
Goals of 5G Standards

Higher data rates





Massive Internet of Things

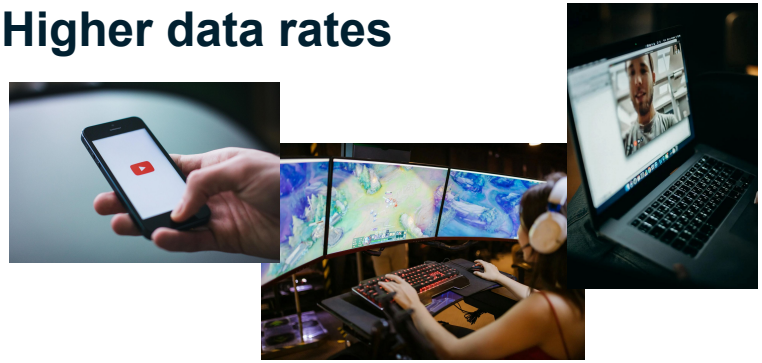


Ultra Reliable & Low Latency

Small Scale & Modular Networks

Goals of 5G Standards

Higher data rates



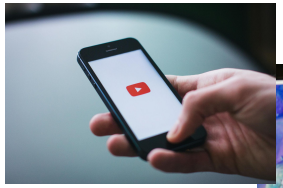
Massive Internet of Things

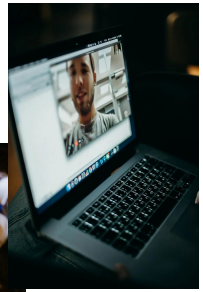
Ultra Reliable & Low Latency

Small Scale & Modular Networks

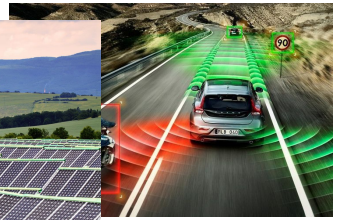
Goals of 5G Standards

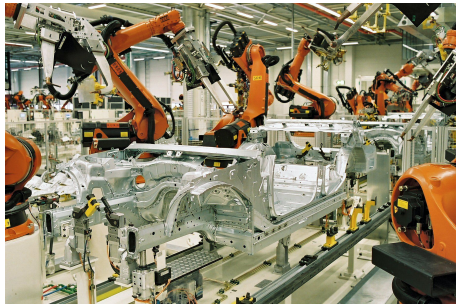
Higher data rates





Massive Internet of Things



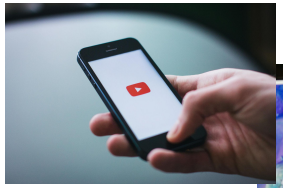


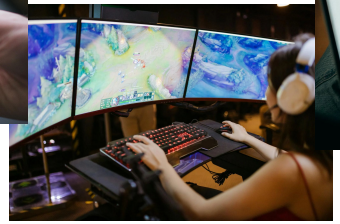
Ultra Reliable & Low Latency

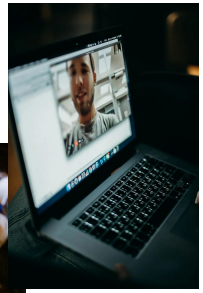
Small Scale & Modular Networks

Goals of 5G Standards

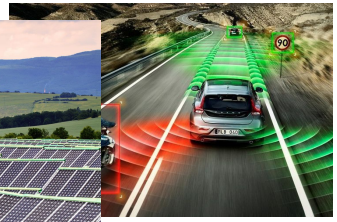
Higher data rates

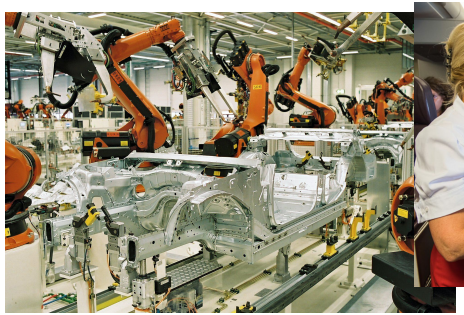






Massive Internet of Things



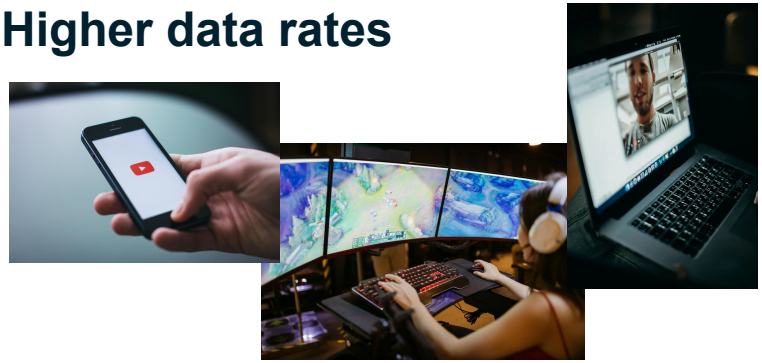


Ultra Reliable & Low Latency

Small Scale & Modular Networks

Goals of 5G Standards

Higher data rates



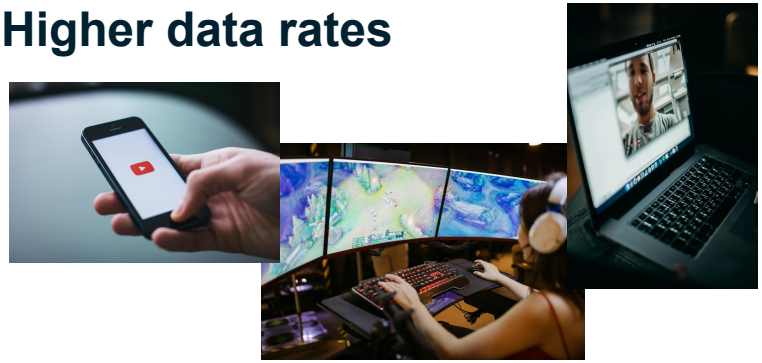
Massive Internet of Things

Ultra Reliable & Low Latency

Small Scale & Modular Networks

Goals of 5G Standards

Higher data rates



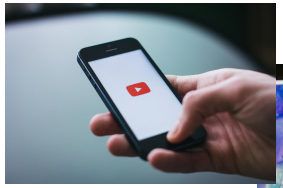
Massive Internet of Things

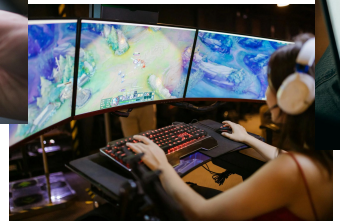
Ultra Reliable & Low Latency

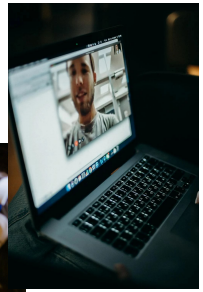
Small Scale & Modular Networks

Goals of 5G Standards

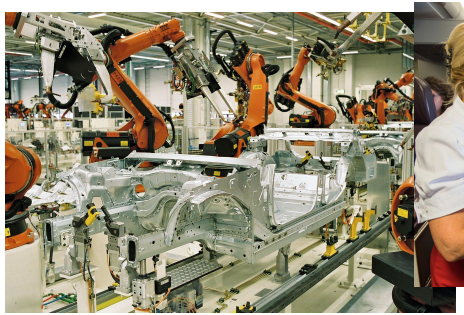
Higher data rates







Massive Internet of Things



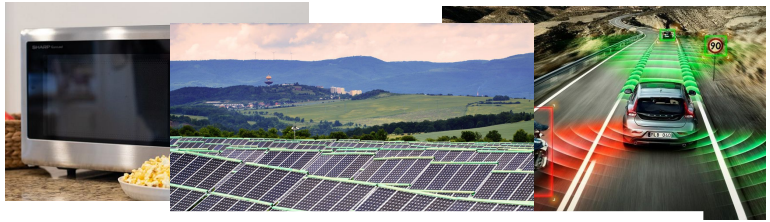
Ultra Reliable & Low Latency

Small Scale & Modula

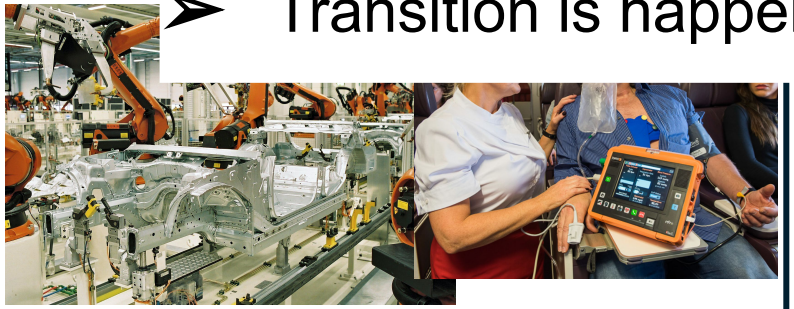
Goals of 5G Standards

Higher data rates

Massive Internet of Things



- 5G is more than just mobile phone networks
- Transition is happening **right now!**



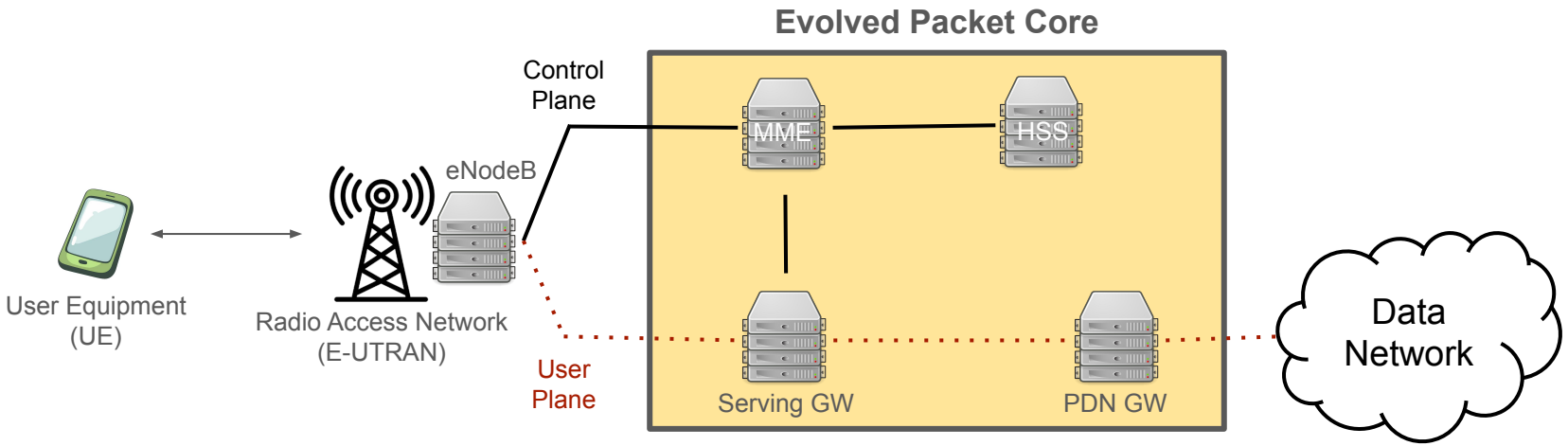
Ultra Reliable & Low Latency

Small Scale & Modula

5G Architecture

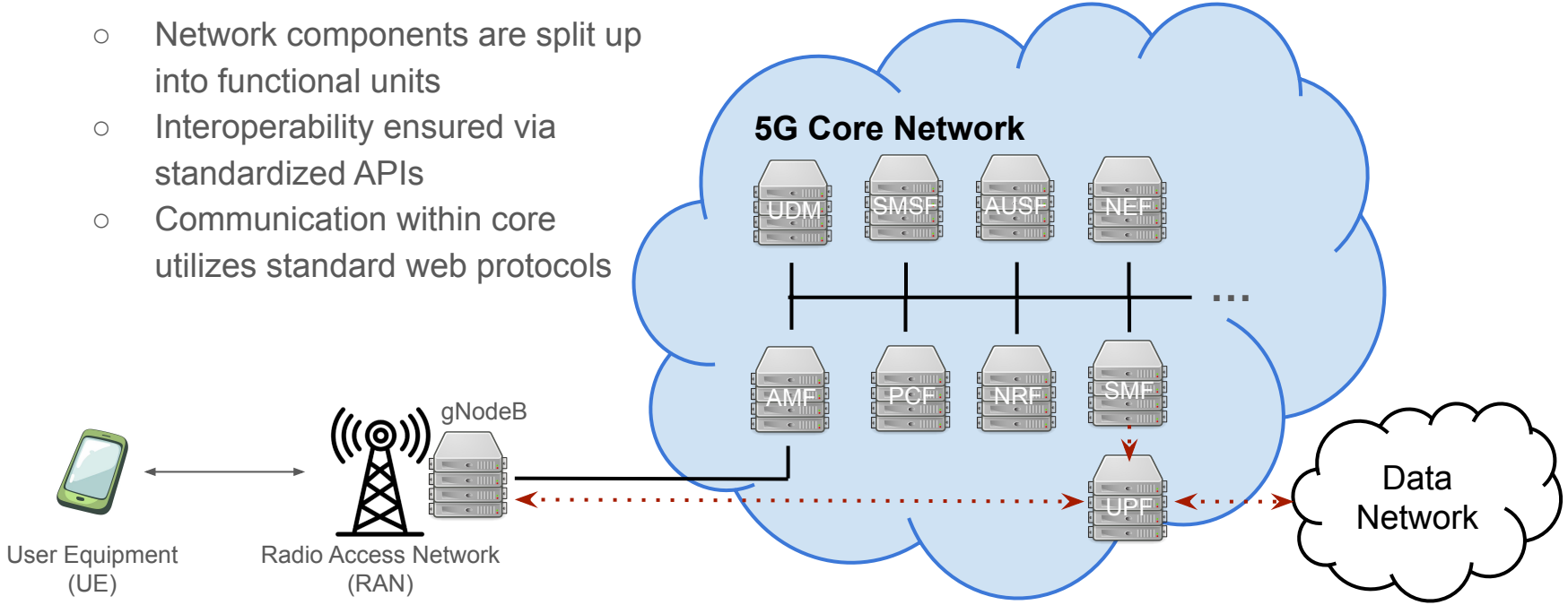
Retrospective: 4G Architecture

- *Big server* somewhere controls network core
- All connections go through *big server*
- Core network technically modular (in theory)

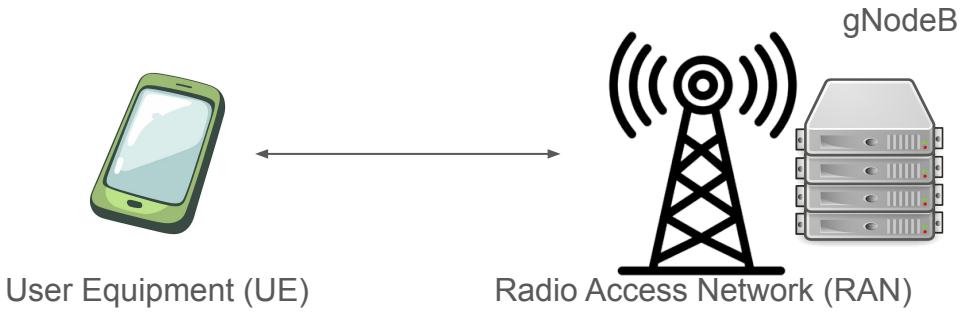


5G and beyond

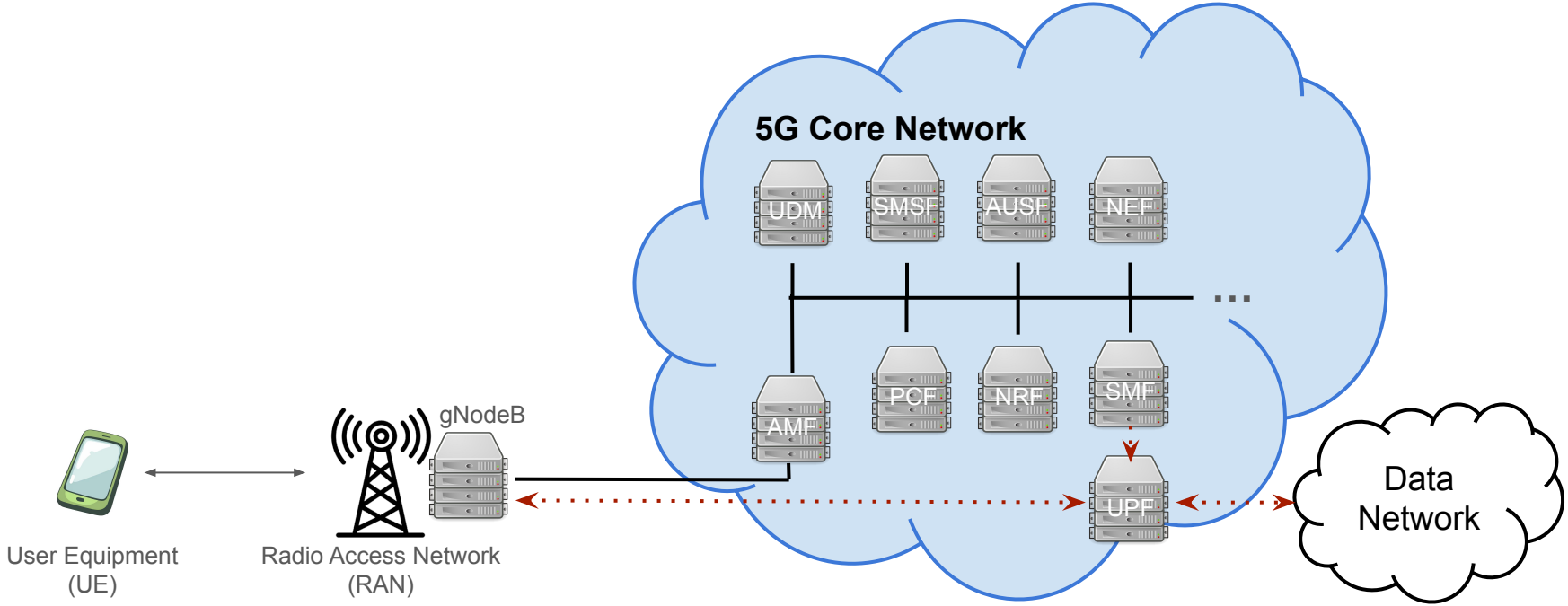
- Modular core architecture
  - Network components are split up into functional units
  - Interoperability ensured via standardized APIs
  - Communication within core utilizes standard web protocols



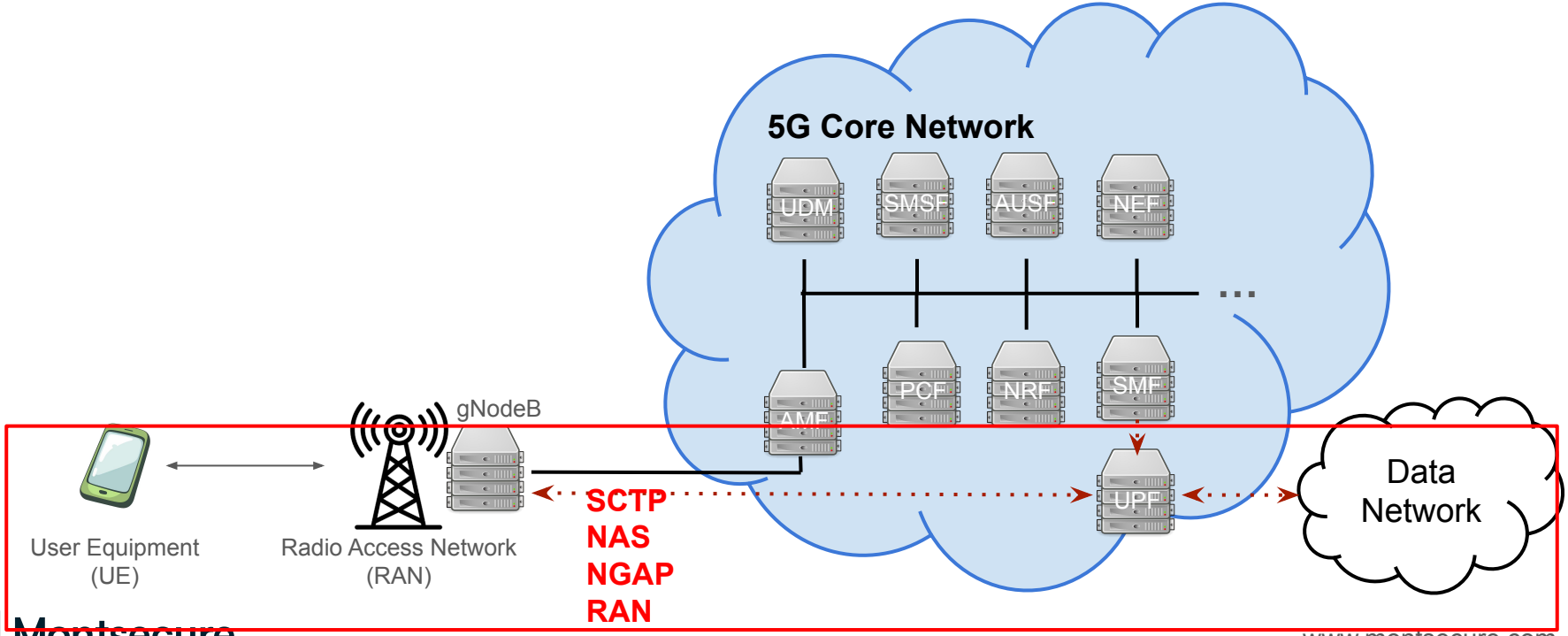
User Equipment -> RAN



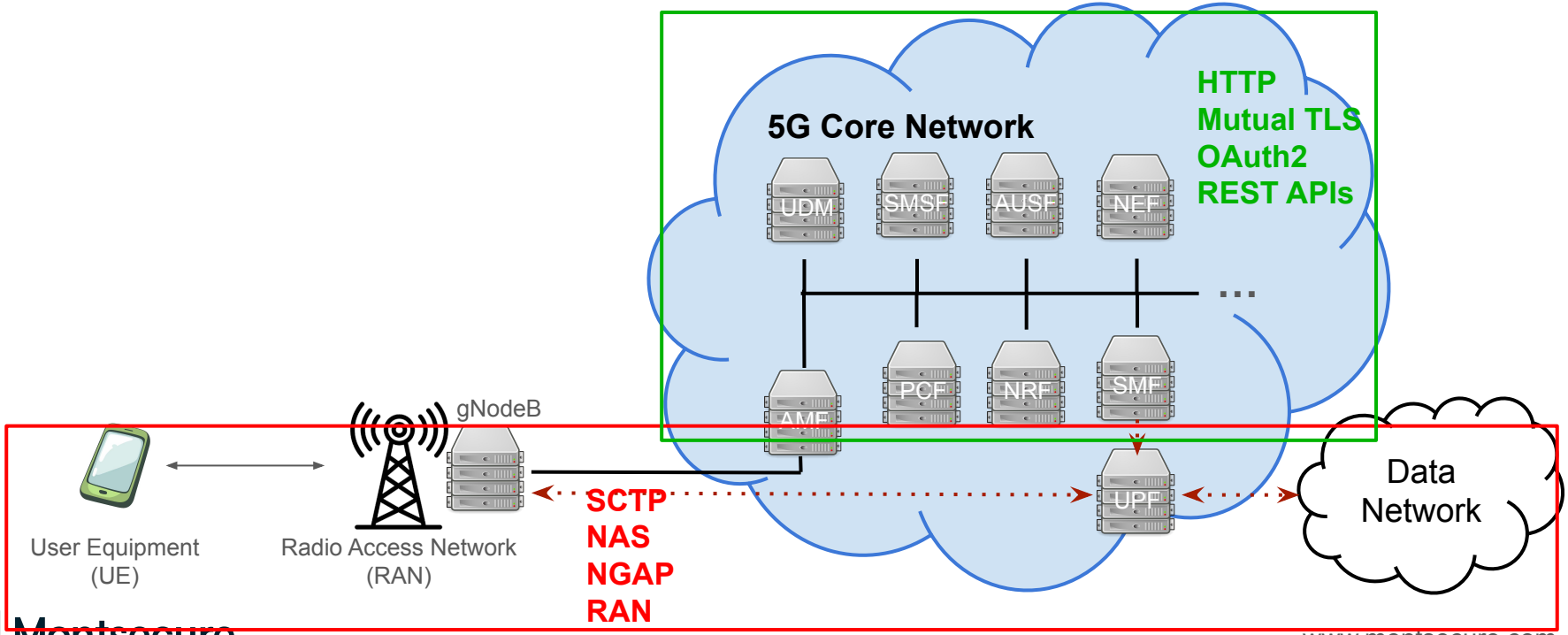
5G Technology Usage



5G Technology Usage

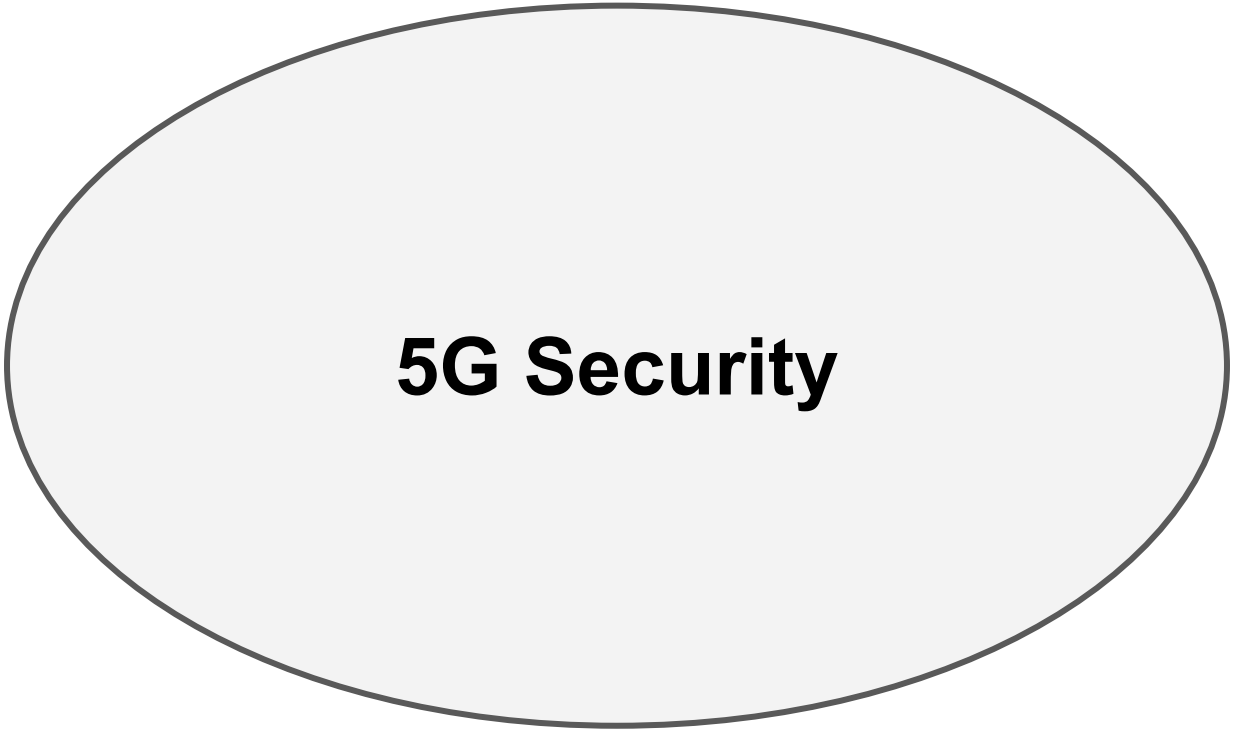


5G Technology Usage

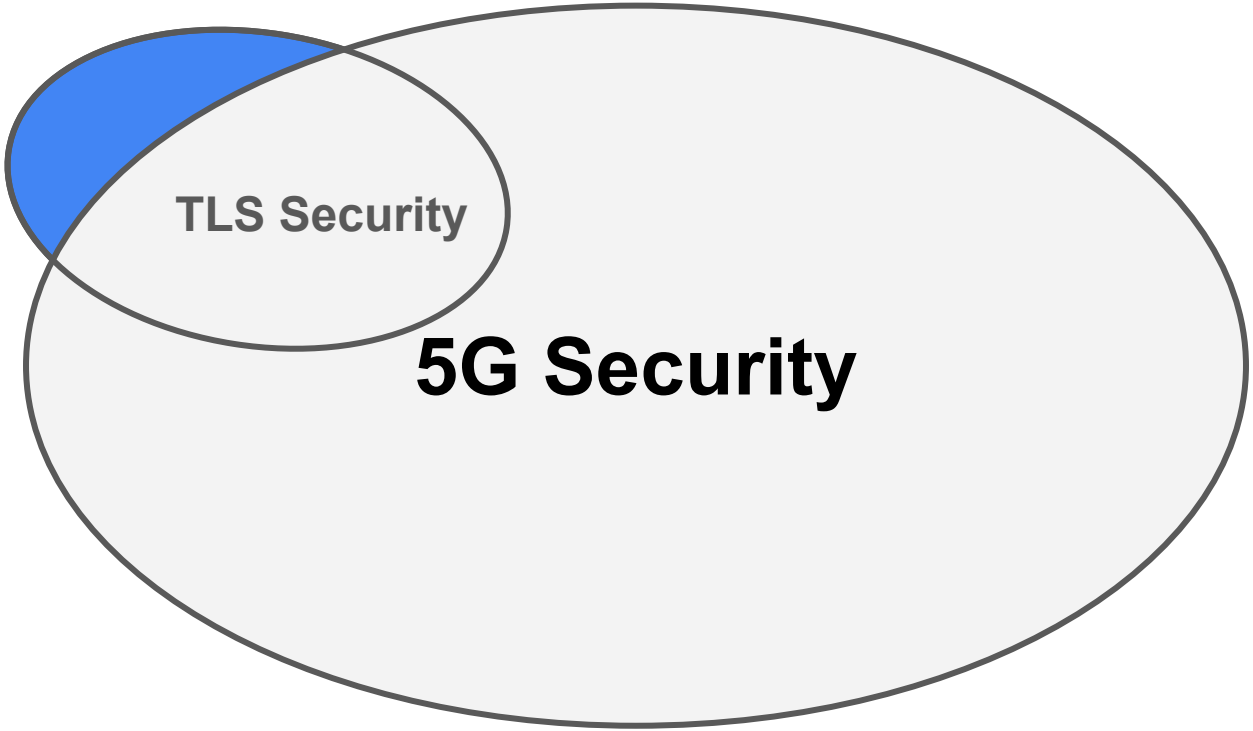


5G Security

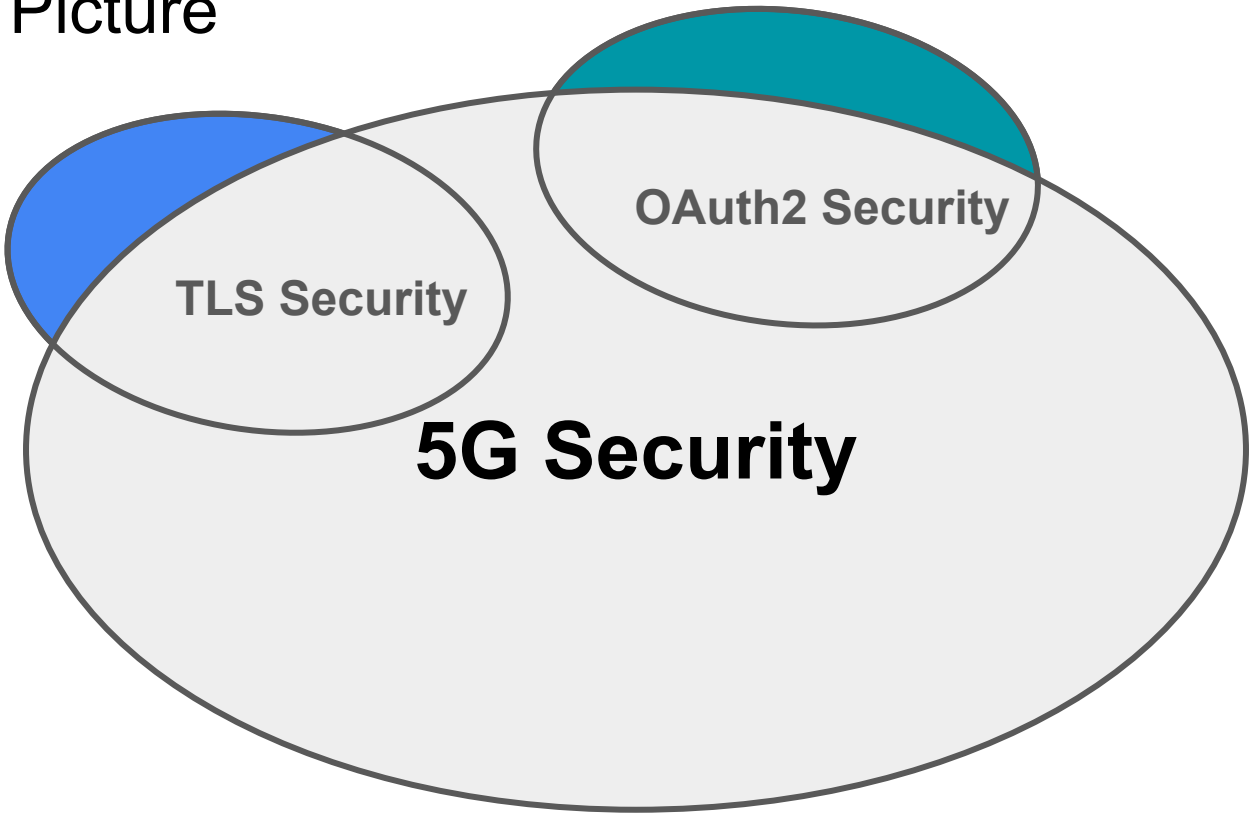
The Big Picture



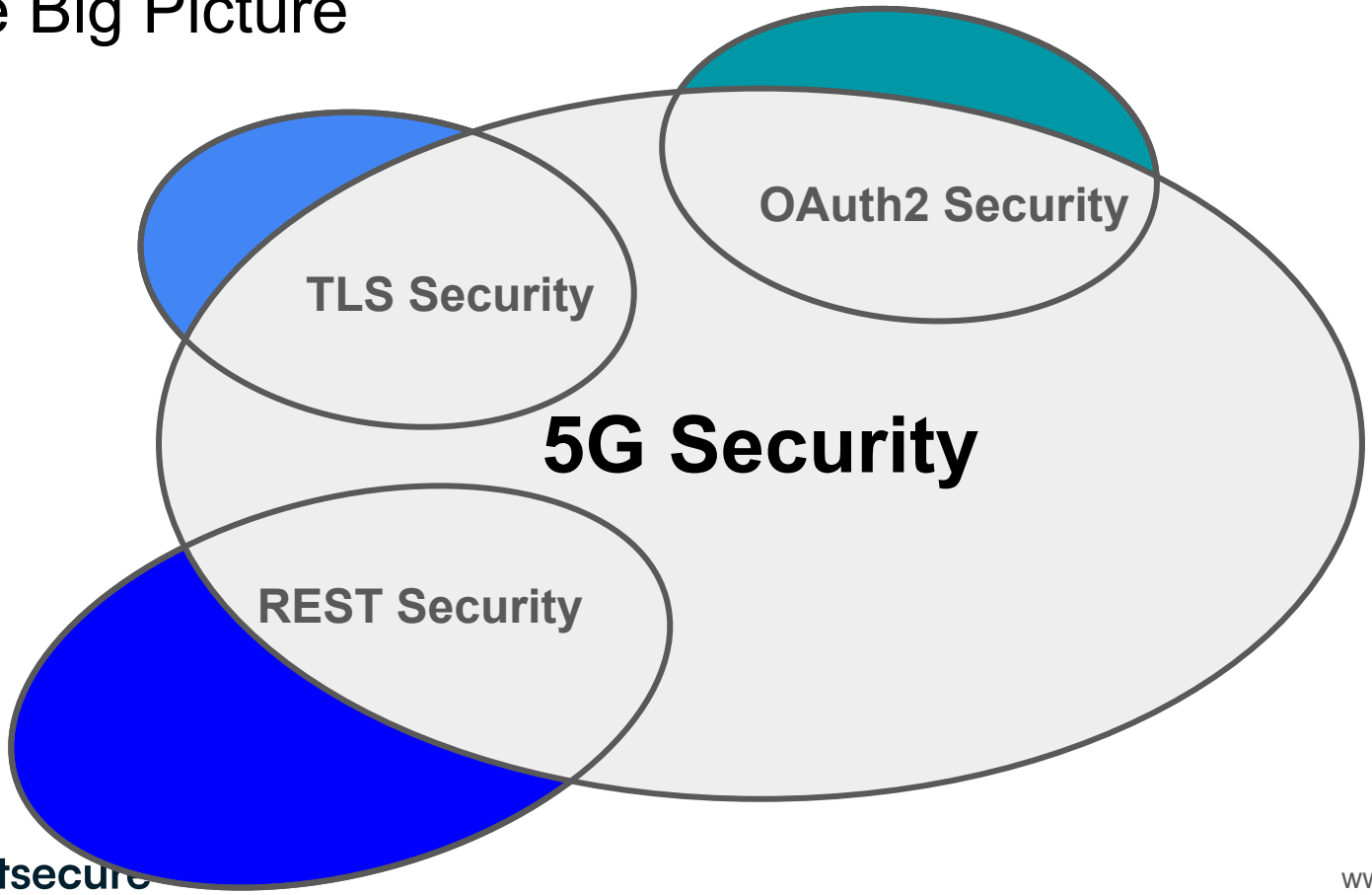
The Big Picture



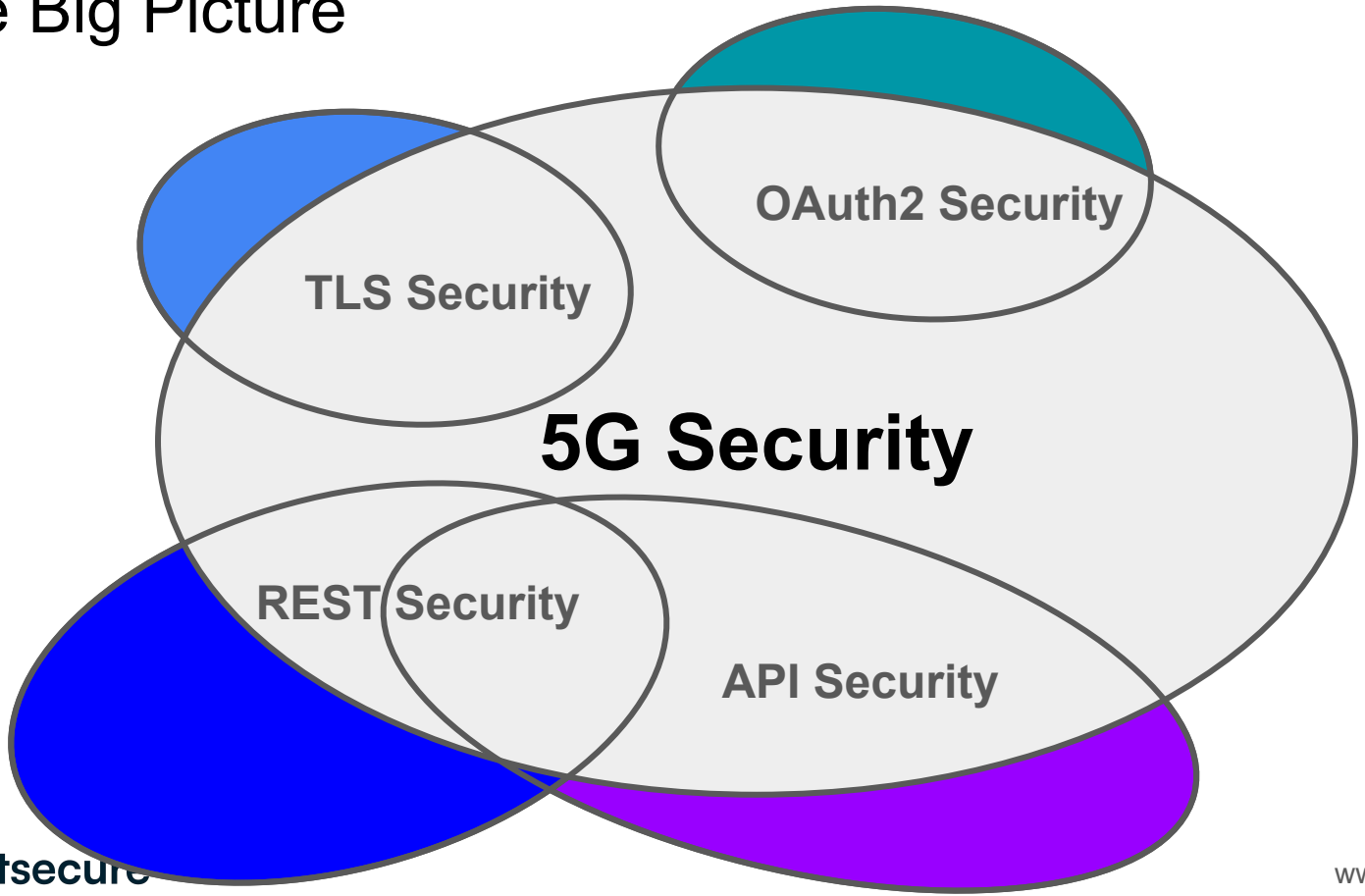
The Big Picture



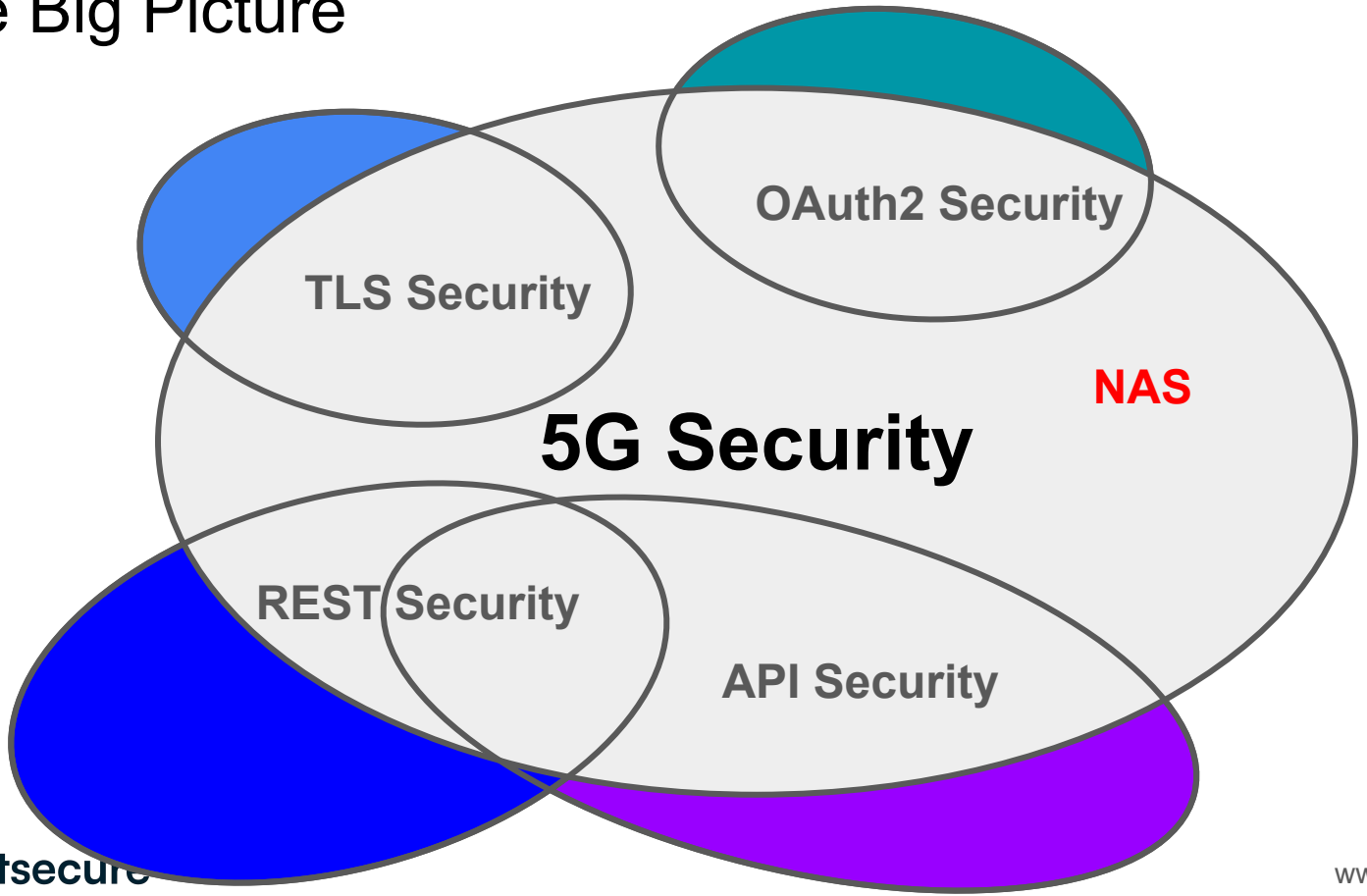
The Big Picture



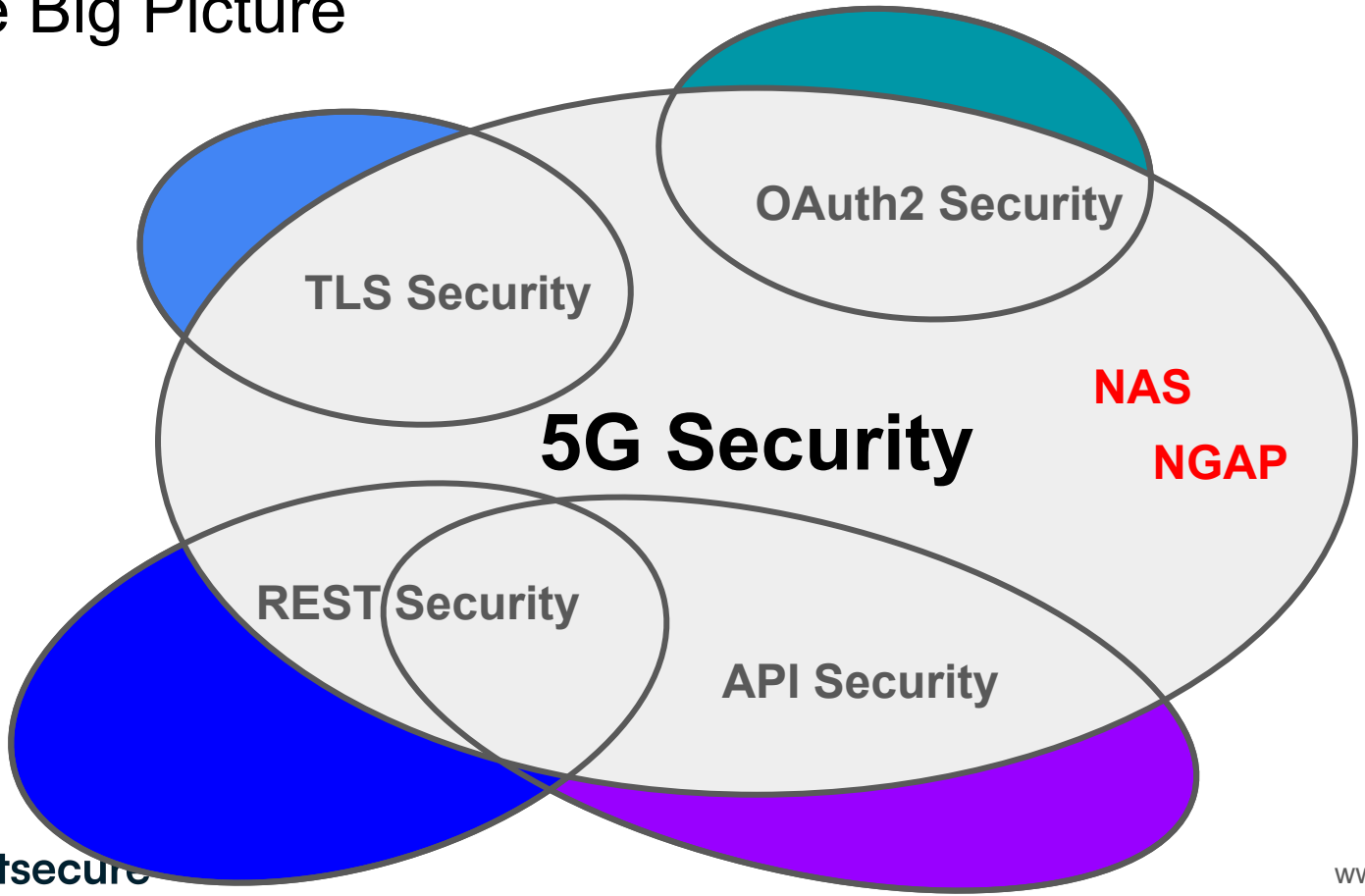
The Big Picture



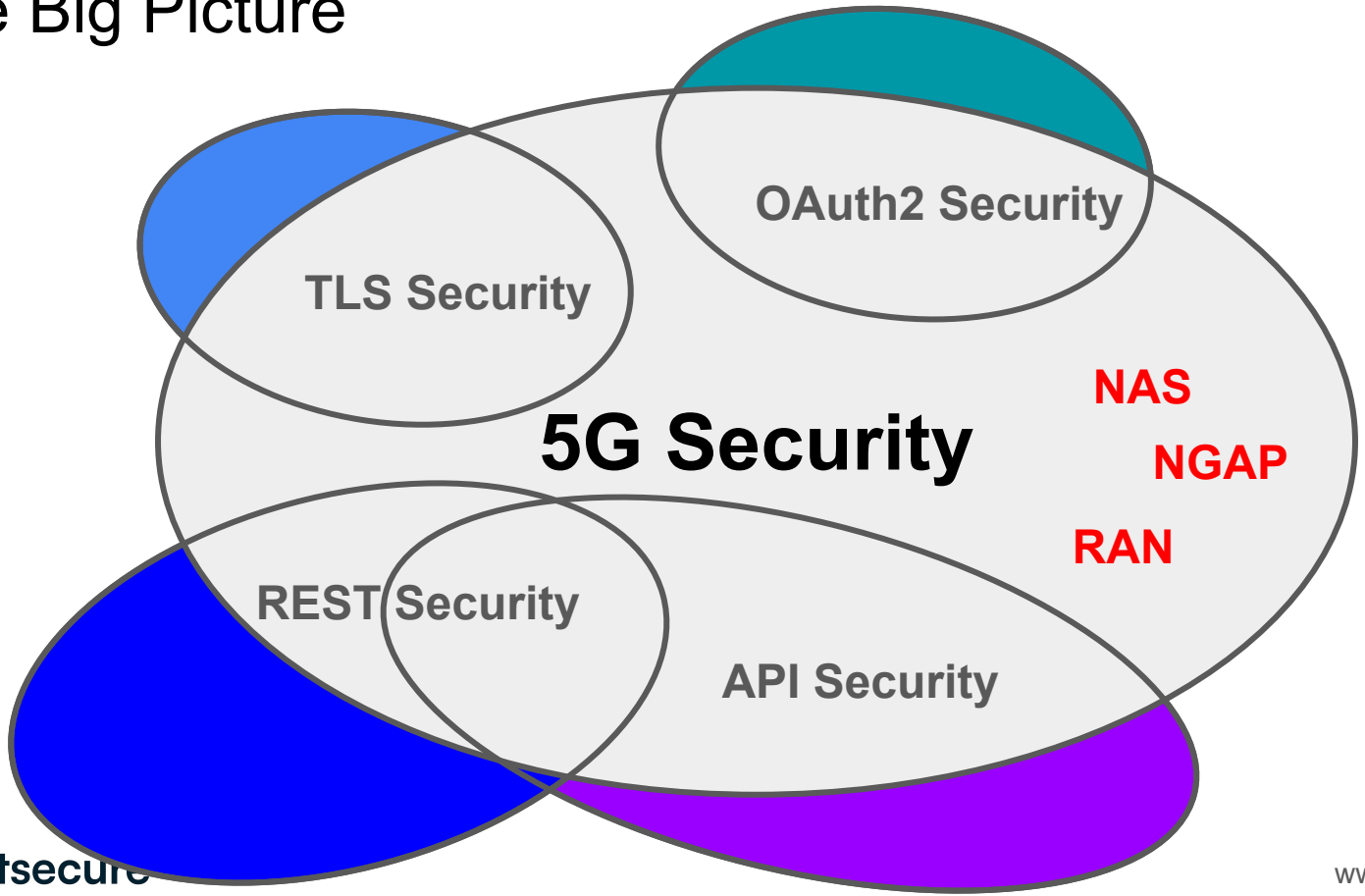
The Big Picture



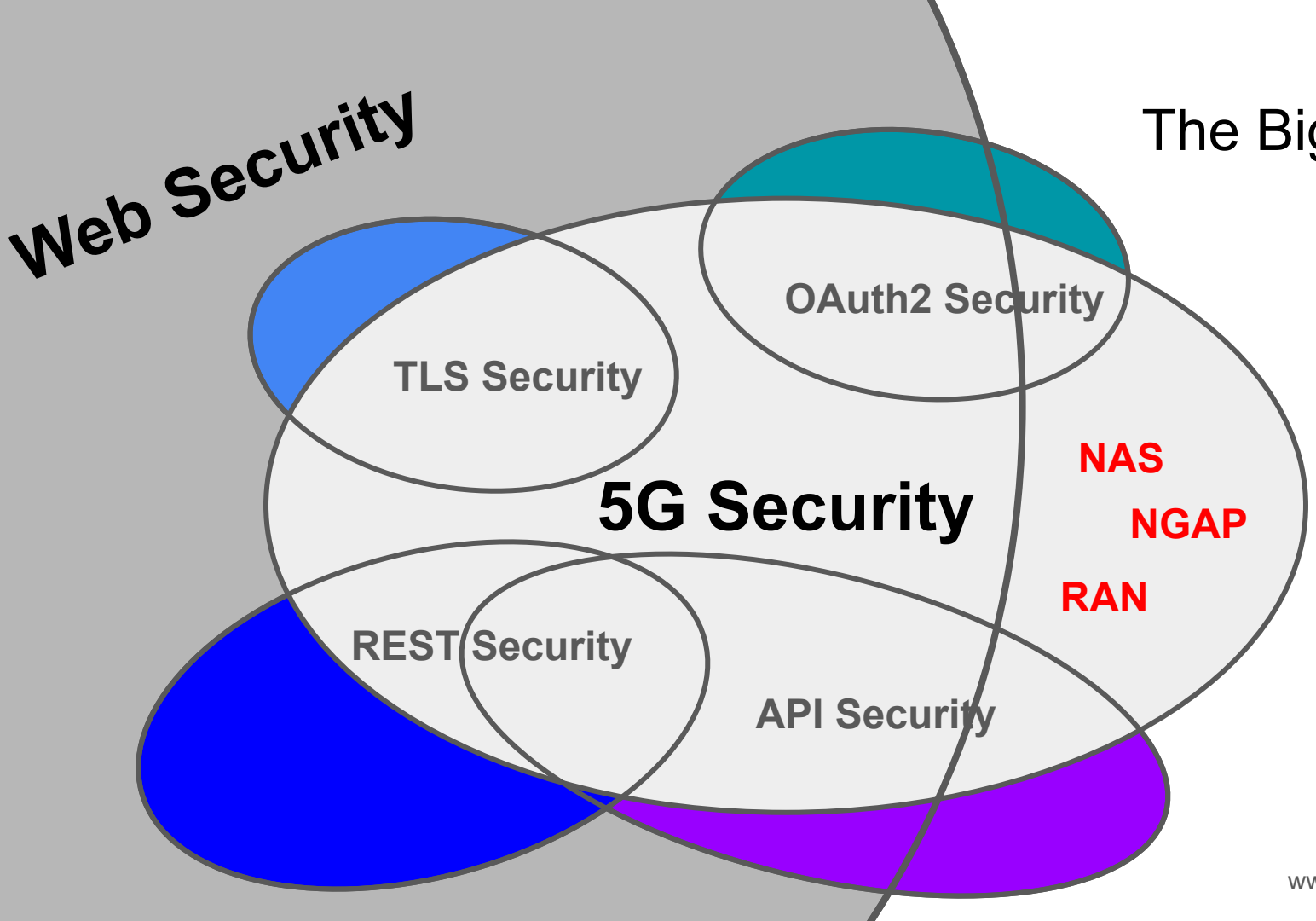
The Big Picture



The Big Picture



The Big Picture



Bridging the Gap

- Can we reuse knowledge from existing web security research?

Bridging the Gap

- Can we reuse knowledge from existing web security research?

  → **Yes!**

Bridging the Gap

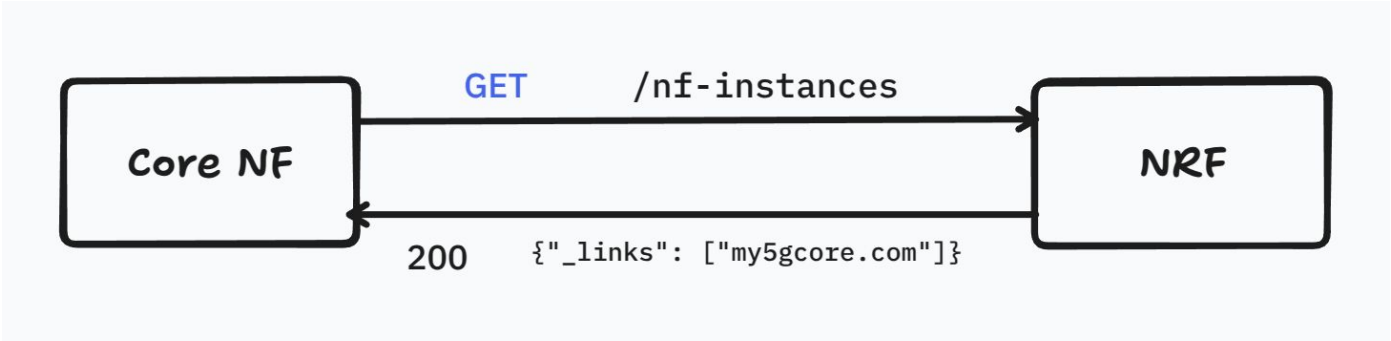
- Can we reuse knowledge from existing web security research?

  → **Yes!***

- *but there are a lot of challenges
  - Navigating complex 5G Architecture
  - Getting access to real-world 5G networks for testing
  - Efficient testing with automation

Example 1: No unused HTTP methods

- Core NFs communicate via 5G REST API interfaces
- HTTP method used in request represents the action performed on an NF resource
- 5G standard defines which action/HTTP methods are allowed for resource



Example 1: No unused HTTP methods

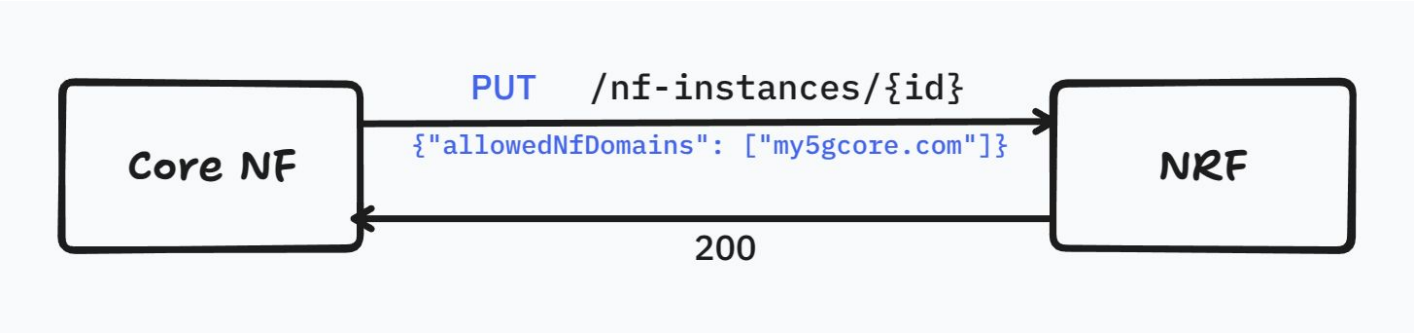
- Attack idea: Modify a read-only resource of an NF

Example 1: No unused HTTP methods

- Result: Resource gets overwritten with attacker's value
  - NF instance data got replaced
  - Possibility for enabling for Machine-In-The-Middle attack

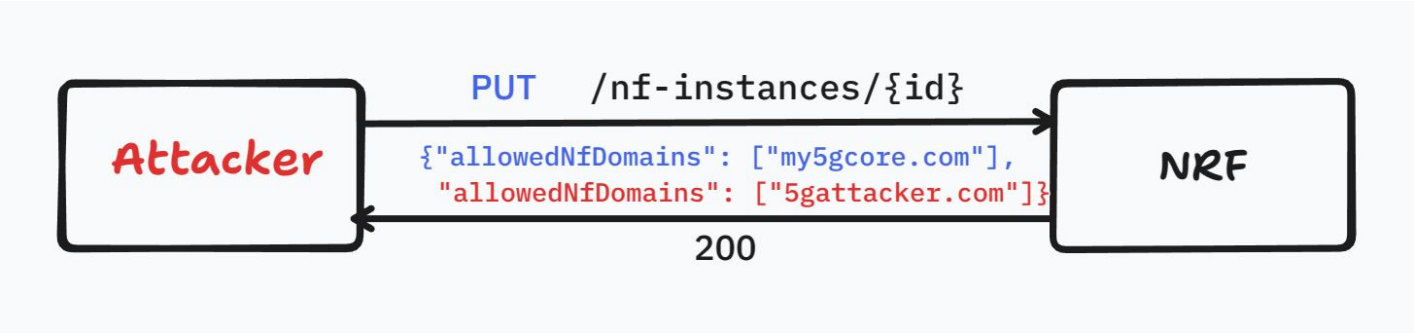
Example 2: No duplicate JSON keys

- API request payloads (usually) are JSON data
- JSON parsers must ensure that received JSON is valid



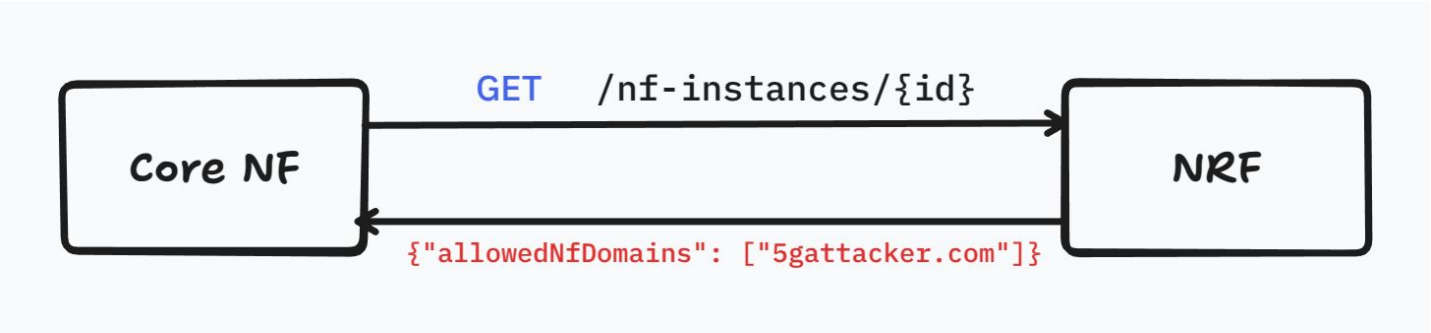
Example 2: No duplicate JSON keys

- Attack idea: Create JSON object where multiple values have same key
  - Which value is read by JSON parser?
  - Can circumvent sanity checks



Example 2: No duplicate JSON keys

- Result: Illegal value may be assigned



Current State of 5G Security

Existing 5G Security Resources

- Official security definitions come from the 3GPP itself
- **Sec**urity **A**ssurance **S**pecification (SCAS)
  - Defined by working group in 3GPP
  - Updated regularly with 3GPP member submissions, e.g. from BSI
    - Minor release ~every quarter
    - Major release ~every year
- Basis for security certification schemes

Cyber certification scheme for network products (EU example)

Existing 5G Security Resources

- Official security definitions come from the 3GPP itself
- **Sec**urity **A**ssurance **S**pecification (SCAS)
  - Defined by working group in 3GPP
  - Updated regularly with 3GPP member submissions, e.g. from BSI
    - Minor release ~every quarter
    - Major release ~every year
- Basis for security certification schemes

Cyber certification scheme for network products (EU example)

Existing 5G Security Resources

- Official security definitions come from the 3GPP itself
- **Sec**urity **A**ssurance **S**pecification (SCAS)
  - Defined by working group in 3GPP
  - Updated regularly with 3GPP member submissions, e.g. from BSI
    - Minor release ~every quarter
    - Major release ~every year
- Basis for security certification schemes

Existing 5G Security Resources

- Official security definitions come from the 3GPP itself
- **S**ec**c**urity **A**ssurance **S**pecification (SCAS)
  - Defined by working group in 3GPP
  - Updated regularly with 3GPP member submissions, e.g. BSI
    - Minor release ~every quarter
    - Major release ~every year
- Basis for security certification schemes
- **Problem**: Submission process is tedious and hopelessly bureaucratic

Excursion: Submission Process (OWASP)

Created JSON Web Encryption Cheat Sheet #1613

Draft **caffeine-rohit** wants to merge 1 commit into `OWASP:master` from `caffeine-rohit:new-JWE-cheat_sheet`

Conversation 20 | Commits 1 | Checks 3 | Files changed 1

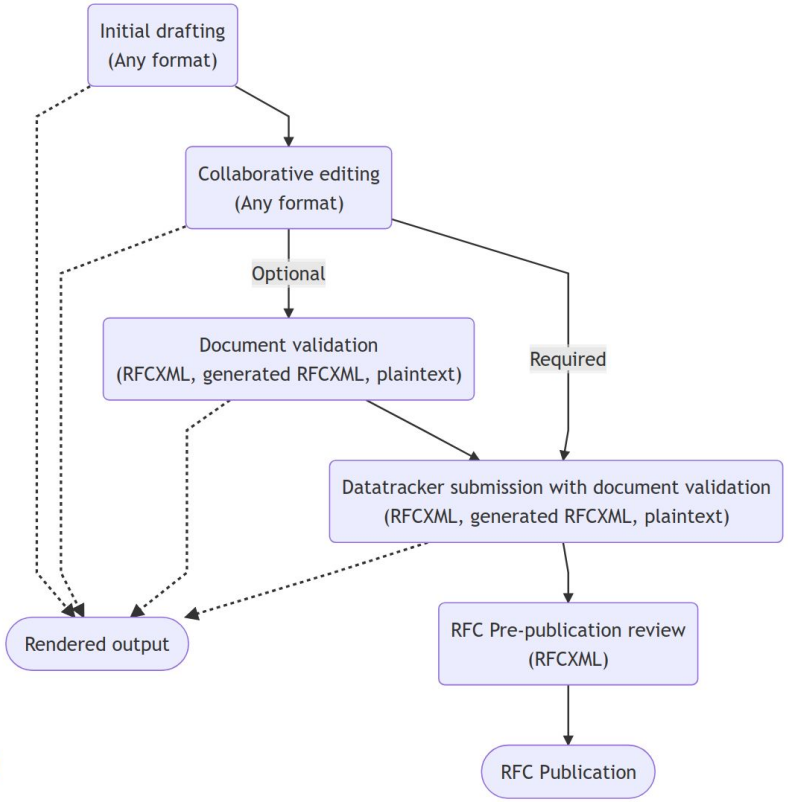
caffeine-rohit commented last week — Contributor

This PR closes #1225 .
This is the draft of the JSON Web Encryption (JWE) Cheat Sheet for the OWASP Cheat Sheet Series.

🔹 Key Highlights:

- 📌 **Introduction to JWE**: Explains its structure, use cases, and differences from JWT.
- 🔐 **Choosing Secure Encryption Algorithms**: Covers AES-GCM, ECDH-ES, RSA-OAEP, and PBES2 with best practices.
- 🛡️ **Implementation Guidelines**: Provides secure encryption and decryption examples in Python & Java.
- ⚠️ **Security Best Practices**:
  - Validation of `alg` and `enc` headers to prevent header manipulation.
  - Proper key management, avoiding nonce/IV reuse, and ensuring AEAD encryption

Excursion: Submission Process (RFC)



Excursion: Submission Process (SCAS) - Step 1

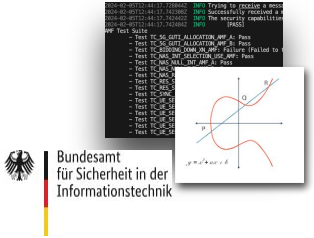
Register at 3GPP →

3GPP™ A GLOBAL INITIATIVE

- Become 3GPP organizational member
  → Pay **2,100€** to become ETSI associate (at minimum)

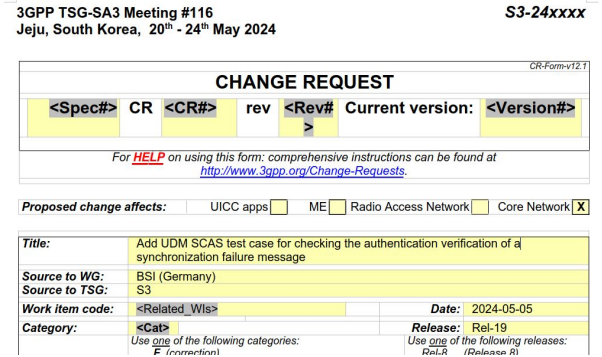
Excursion: Submission Process (SCAS) - Step 2

Research Data



Create a Change Request (CR)

- Fill out Microsoft™ Word™ .doc template



3GPP TSG-SA3 Meeting #116 — S3-24xxxx
Jeju, South Korea, 20th - 24th May 2024

CR-Form-v12.1

CHANGE REQUEST

<Spec#>	CR	<CR#>	rev	<Rev#>	Current version:	<Version#>

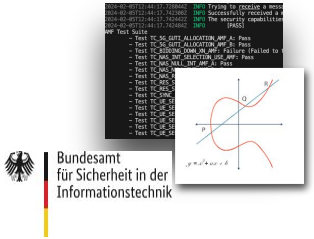
For HELP on using this form: comprehensive instructions can be found at http://www.3gpp.org/Change-Requests.

Proposed change affects:	UICC apps ☐	ME ☐	Radio Access Network ☐	Core Network ☒

Title:	Add UDM SCAS test case for checking the authentication verification of a synchronization failure message		
Source to WG:	BSI (Germany)		
Source to TSG:	S3		
Work item code:	<Related_WIs>	***Date:***	2024-05-05
Category:	<Cat>	***Release:***	Rel-19
	Use one of the following categories: F (correction)	*Use one of the following releases:* Rel-8 (Release 8)	

Excursion: Submission Process (SCAS) - Step 2

Research Data



Create a Change Request (CR)

- Fill out Microsoft™ Word™ .doc template

********** START OF 1st CHANGE **********

H.2.2.1 No slice specific authorization for NF discovery

- *Threat name*: No slice specific authorization for NF discovery.
- *Threat Category*: Information Disclosure, Elevation of privilege.
- *Threat Description:* If NF discovery authorization for specific slice is not supported by the NRF, the NF instance in one slice can discover NF instances belonging to other slices. This can result in reduced assurance level of slice data isolation, making the system easily attacked as well as wasting resource.
- *Threatened asset:* NF profile of available NF instances.

********** END OF CHANGE **********

Excursion: Submission Process (SCAS) - Step 3

Upload Change Request (CR)

3GPP™
A GLOBAL INITIATIVE

- Submit change request to 3GPP portal
- Wait for feedback

Excursion: Submission Process (SCAS) - Step 3

Upload Change Request (CR)

3GPP™
A GLOBAL INITIATIVE

- Submit change request to 3GPP portal
- Wait for feedback

Excursion: Submission Process (SCAS) - Step 3

Upload Change Request (CR)

3GPP™
A GLOBAL INITIATIVE

- Submit change request to 3GPP portal
- Wait for feedback

Excursion: Submission Process (SCAS) - Step 3

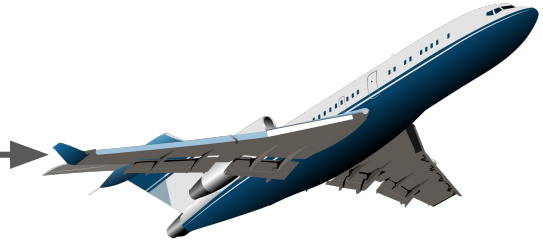
Upload Change Request (CR)

3GPP™
A GLOBAL INITIATIVE

- Submit change request to 3GPP portal
- ~~Wait for feedback~~

Excursion: Submission Process (SCAS) - Step 4

Get onto a plane



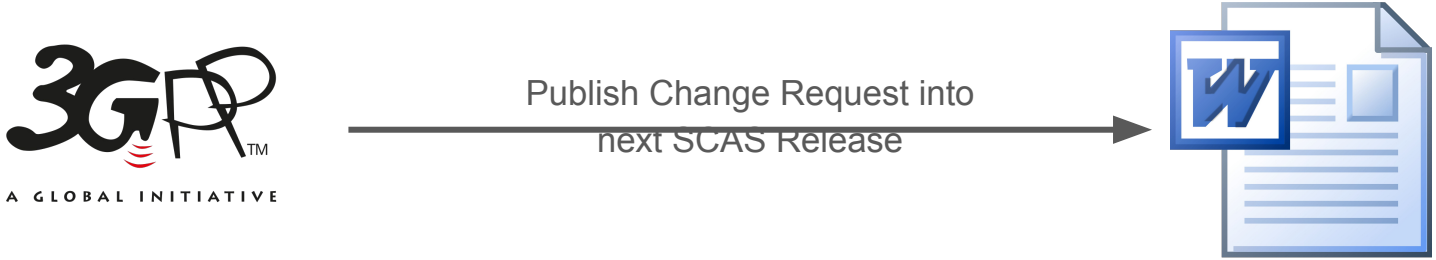
- Fly across the globe to 3GPP plenary meetings (every 3 months)

Excursion: Submission Process (SCAS) - Step 5

Talk to 3GPP members →

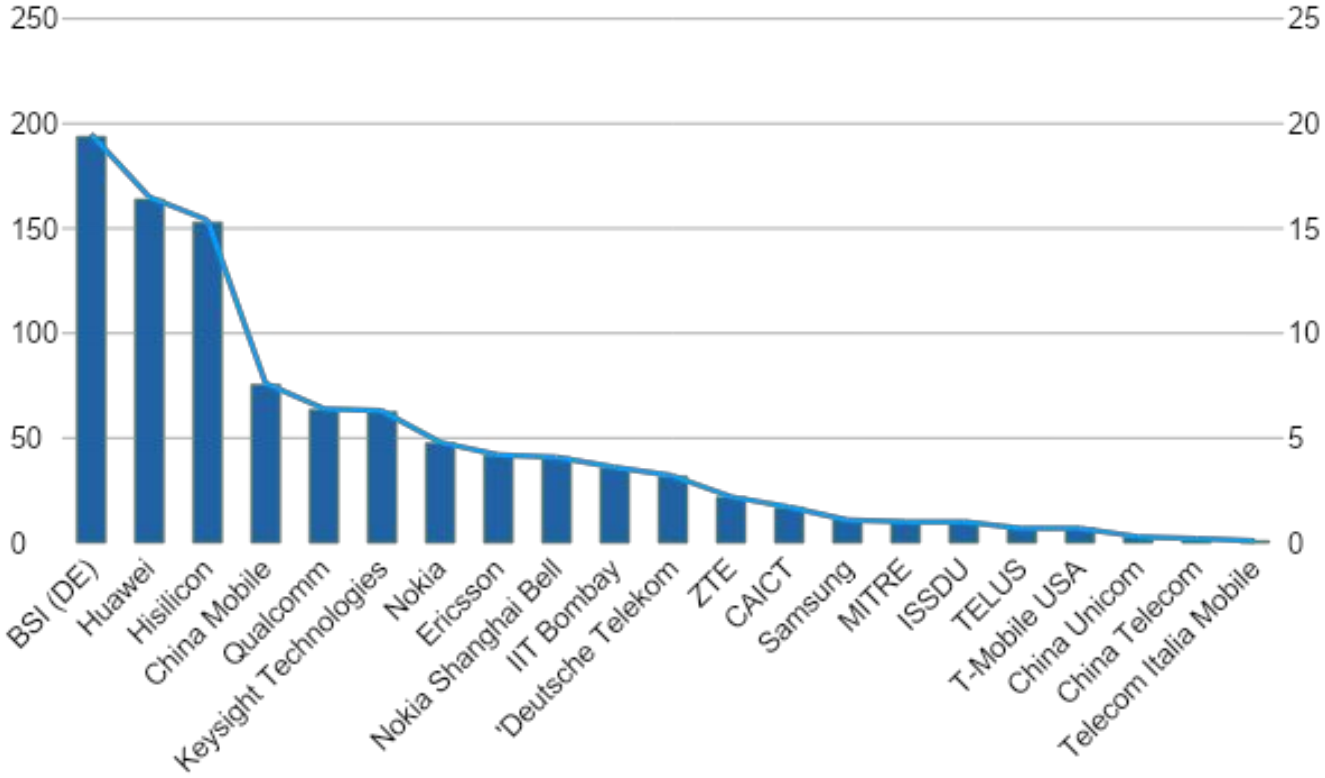
- Prepare to negotiate change request with other 3GPP members → otherwise your CR may not be accepted!
- Hope that your change request gets approved

Excursion: Submission Process (SCAS) - Step 6



- Approved change requests get integrated into next SCAS release
- Uploaded to 3GPP Portal (as Microsoft™ Word™ documents)

Excursion: SCAS Submission Statistics (August 2024)



Future Outlook

5G certification scheme in Germany

- Certification becomes mandatory starting in 2026
- Targets public 5G network *products*
- Certification efforts have just started

→ Big question: Can all networks be certified by 2026?

Thank You!