THE EU CYBERSECURITY AGENCY

ENISA 5G SECURITY CONTROLS MATRIX

Sławomir Bryska

Policy Development and Implementation Unit, ENISA

OUR GOAL

To consolidate various 5G security controls in a single repository

Numerous sources of information relevant to 5G security

3GPP

ISO

ETSI

NIST

IETF

ITU

eTOM

Benefit to NRAs, telecom companies and others stakeholders

5G

5G Security Controls Matrix

powered by ENISA

THE CONTENTS SO FAR

GUIDELINE ON SECURITY MEASURES UNDER THE EECC

3rd Edition

DECEMBER 2020

8 security domains

29 security objectives

144 high level measures

+ evidence

339 detailed controls

+ evidence

Mapping with standards, specifications, frameworks and guidelines

Mapping with assets

5G SUPPLEMENT

To the Guideline on Security Measures under the EECC

DECEMBER 2020

ENISA THREAT LANDSCAPE FOR 5G NETWORKS

Updated threat assessment for the fifth generation of mobile telecommunications networks (5G)

DECEMBER 2020

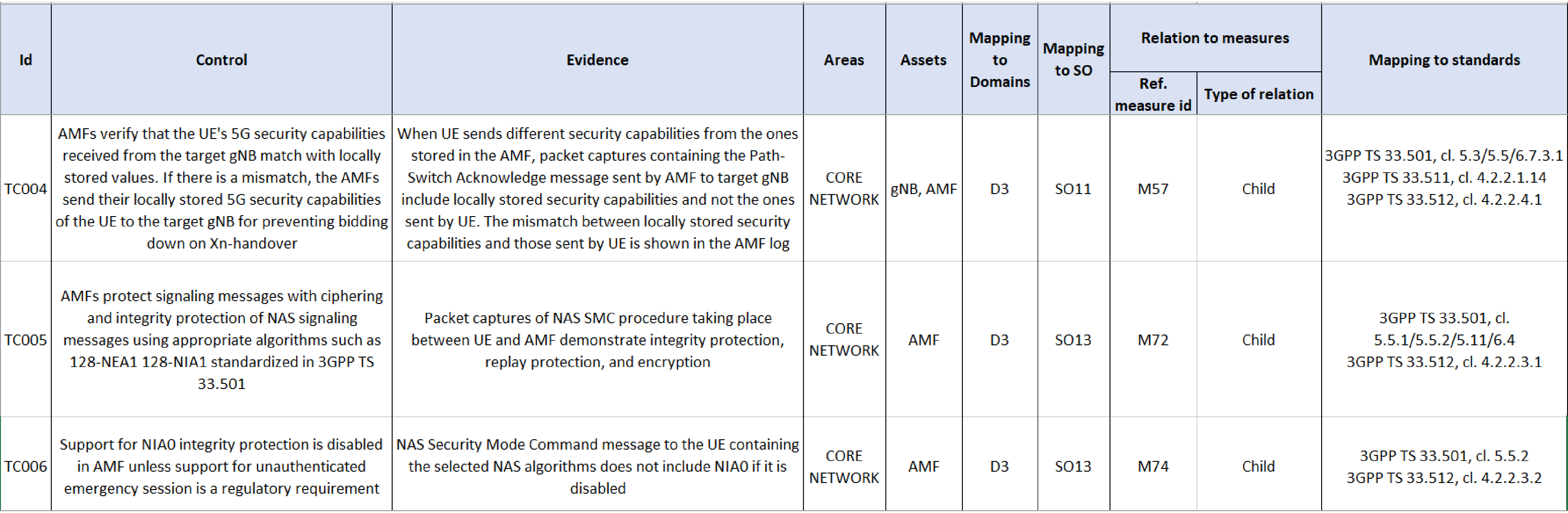
SECURITY IN 5G SPECIFICATIONS

Controls in 3GPP Security Specifications (5G SA)

FEBRUARY 2021

Additional specs not captured in the documents to the left

DETAILED SECURITY CONTROLS - OVERVIEW

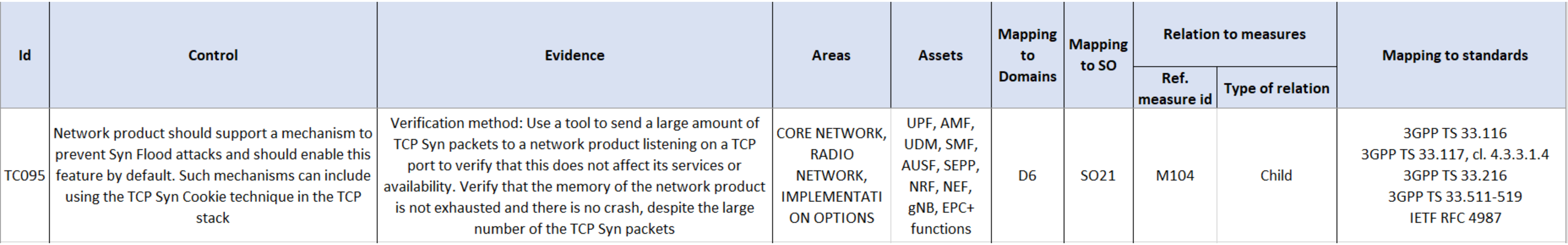


Id	Control	Evidence	Areas	Assets	Mapping to Domains	Mapping to SO	Relation to measures		Mapping to standards
							Ref. measure id	Type of relation	
TC004	AMFs verify that the UE's 5G security capabilities received from the target gNB match with locally stored values. If there is a mismatch, the AMFs send their locally stored 5G security capabilities of the UE to the target gNB for preventing bidding down on Xn-handover	When UE sends different security capabilities from the ones stored in the AMF, packet captures containing the Path-Switch Acknowledge message sent by AMF to target gNB include locally stored security capabilities and not the ones sent by UE. The mismatch between locally stored security capabilities and those sent by UE is shown in the AMF log	CORE NETWORK	gNB, AMF	D3	SO11	M57	Child	3GPP TS 33.501, cl. 5.3/5.5/6.7.3.1 3GPP TS 33.511, cl. 4.2.2.1.14 3GPP TS 33.512, cl. 4.2.2.4.1
TC005	AMFs protect signaling messages with ciphering and integrity protection of NAS signaling messages using appropriate algorithms such as 128-NEA1 128-NIA1 standardized in 3GPP TS 33.501	Packet captures of NAS SMC procedure taking place between UE and AMF demonstrate integrity protection, replay protection, and encryption	CORE NETWORK	AMF	D3	SO13	M72	Child	3GPP TS 33.501, cl. 5.5.1/5.5.2/5.11/6.4 3GPP TS 33.512, cl. 4.2.2.3.1
TC006	Support for NIA0 integrity protection is disabled in AMF unless support for unauthenticated emergency session is a regulatory requirement	NAS Security Mode Command message to the UE containing the selected NAS algorithms does not include NIA0 if it is disabled	CORE NETWORK	AMF	D3	SO13	M74	Child	3GPP TS 33.501, cl. 5.5.2 3GPP TS 33.512, cl. 4.2.2.3.2

Extract

DETAILED SECURITY CONTROLS - EVIDENCE

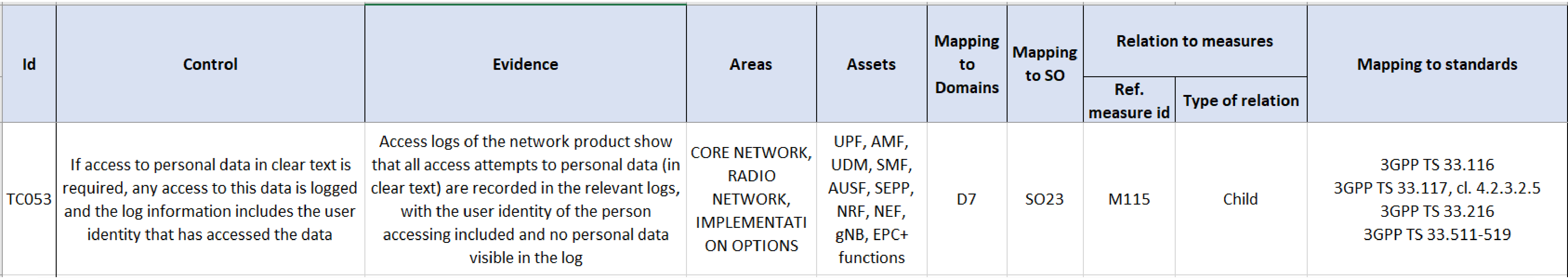
As appropriate, evidence descriptions take the form of testing methods…



Id	Control	Evidence	Areas	Assets	Mapping to Domains	Mapping to SO	Relation to measures		Mapping to standards
							Ref. measure id	Type of relation	
TC095	Network product should support a mechanism to prevent Syn Flood attacks and should enable this feature by default. Such mechanisms can include using the TCP Syn Cookie technique in the TCP stack	Verification method: Use a tool to send a large amount of TCP Syn packets to a network product listening on a TCP port to verify that this does not affect its services or availability. Verify that the memory of the network product is not exhausted and there is no crash, despite the large number of the TCP Syn packets	CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS	UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	D6	SO21	M104	Child	3GPP TS 33.116 3GPP TS 33.117, cl. 4.3.3.1.4 3GPP TS 33.216 3GPP TS 33.511-519 IETF RFC 4987

Extract

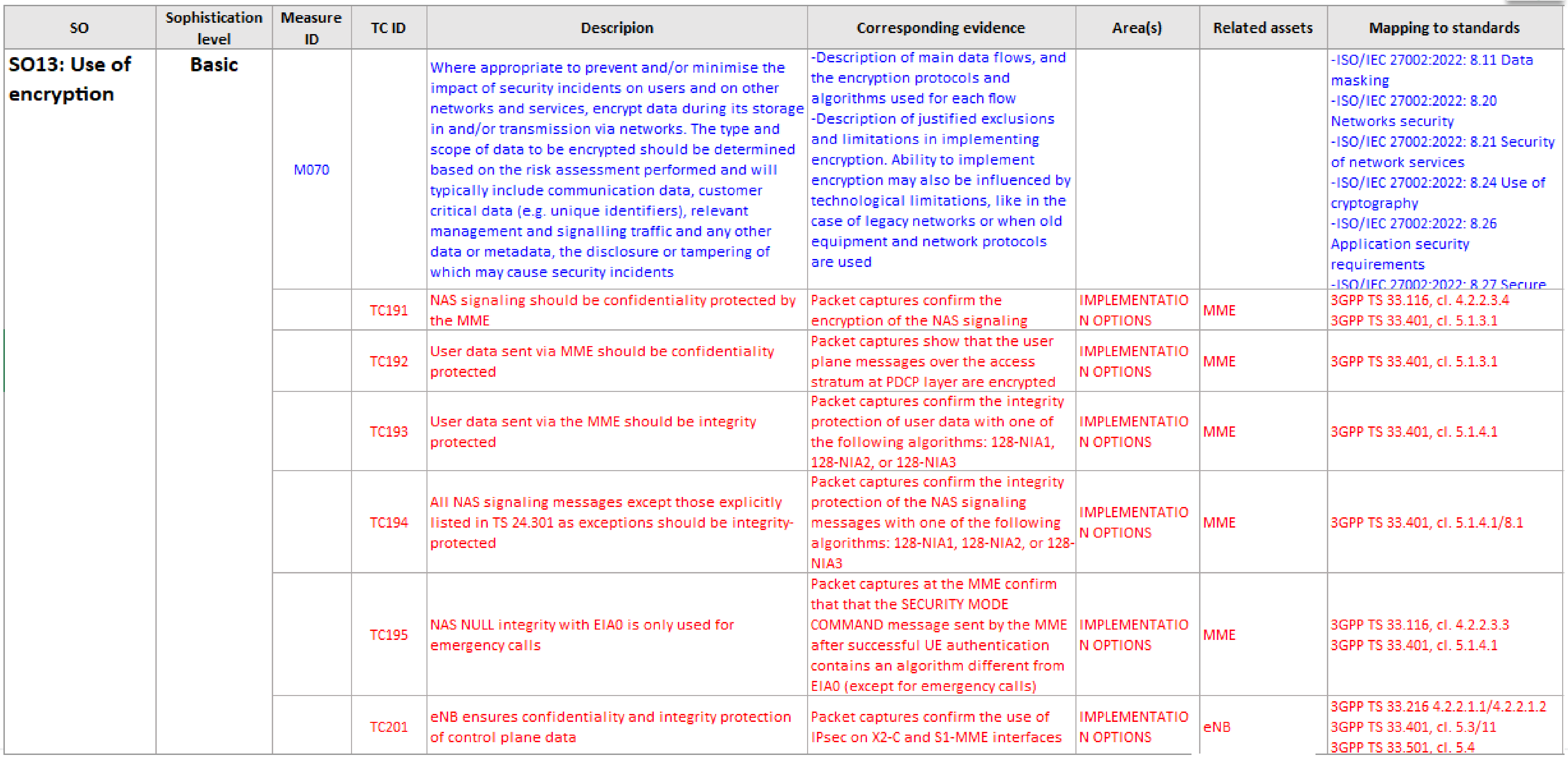
…or documented information.



Id	Control	Evidence	Areas	Assets	Mapping to Domains	Mapping to SO	Relation to measures		Mapping to standards
							Ref. measure id	Type of relation	
TC053	If access to personal data in clear text is required, any access to this data is logged and the log information includes the user identity that has accessed the data	Access logs of the network product show that all access attempts to personal data (in clear text) are recorded in the relevant logs, with the user identity of the person accessing included and no personal data visible in the log	CORE NETWORK, RADIO NETWORK, IMPLEMENTATION OPTIONS	UPF, AMF, UDM, SMF, AUSF, SEPP, NRF, NEF, gNB, EPC+ functions	D7	SO23	M115	Child	3GPP TS 33.116 3GPP TS 33.117, cl. 4.2.3.2.5 3GPP TS 33.216 3GPP TS 33.511-519

Extract

THREE WAYS TO PRESENT ALL THE CONTROLS

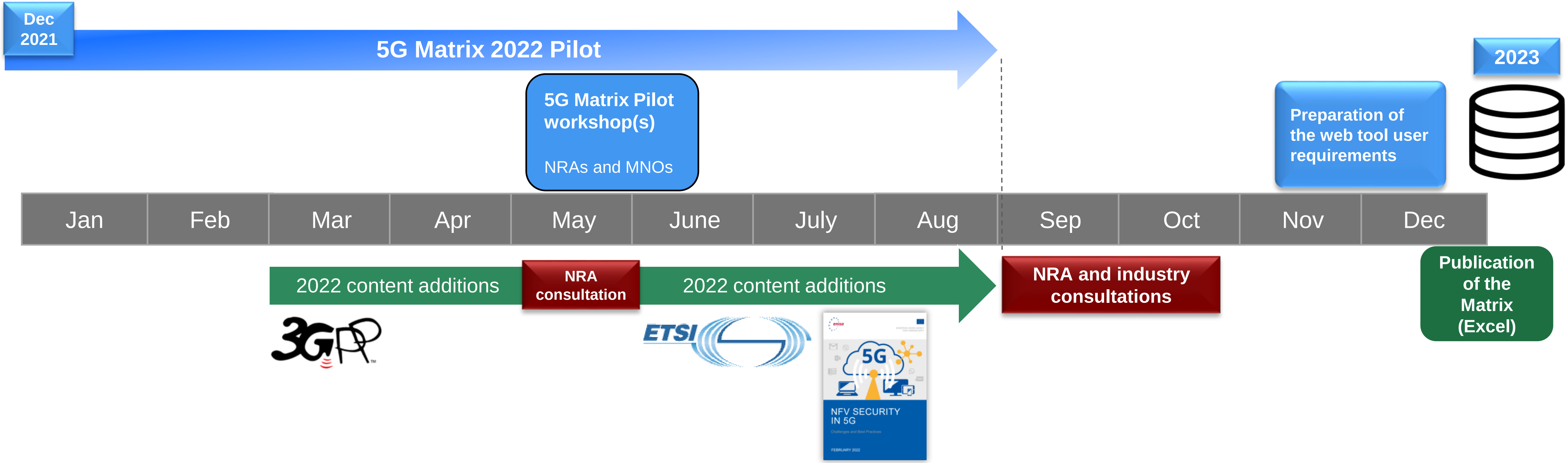


SO	Sophistication level	Measure ID	TC ID	Description	Corresponding evidence	Area(s)	Related assets	Mapping to standards
SO13: Use of encryption	**Basic**	M070		Where appropriate to prevent and/or minimise the impact of security incidents on users and on other networks and services, encrypt data during its storage in and/or transmission via networks. The type and scope of data to be encrypted should be determined based on the risk assessment performed and will typically include communication data, customer critical data (e.g. unique identifiers), relevant management and signalling traffic and any other data or metadata, the disclosure or tampering of which may cause security incidents	-Description of main data flows, and the encryption protocols and algorithms used for each flow -Description of justified exclusions and limitations in implementing encryption. Ability to implement encryption may also be influenced by technological limitations, like in the case of legacy networks or when old equipment and network protocols are used			-ISO/IEC 27002:2022: 8.11 Data masking -ISO/IEC 27002:2022: 8.20 Networks security -ISO/IEC 27002:2022: 8.21 Security of network services -ISO/IEC 27002:2022: 8.24 Use of cryptography -ISO/IEC 27002:2022: 8.26 Application security requirements -ISO/IEC 27002:2022: 8.27 Secure
			TC191	NAS signaling should be confidentiality protected by the MME	Packet captures confirm the encryption of the NAS signaling	IMPLEMENTATION OPTIONS	MME	3GPP TS 33.116, cl. 4.2.2.3.4 3GPP TS 33.401, cl. 5.1.3.1
			TC192	User data sent via MME should be confidentiality protected	Packet captures show that the user plane messages over the access stratum at PDCP layer are encrypted	IMPLEMENTATION OPTIONS	MME	3GPP TS 33.401, cl. 5.1.3.1
			TC193	User data sent via the MME should be integrity protected	Packet captures confirm the integrity protection of user data with one of the following algorithms: 128-NIA1, 128-NIA2, or 128-NIA3	IMPLEMENTATION OPTIONS	MME	3GPP TS 33.401, cl. 5.1.4.1
			TC194	All NAS signaling messages except those explicitly listed in TS 24.301 as exceptions should be integrity-protected	Packet captures confirm the integrity protection of the NAS signaling messages with one of the following algorithms: 128-NIA1, 128-NIA2, or 128-NIA3	IMPLEMENTATION OPTIONS	MME	3GPP TS 33.401, cl. 5.1.4.1/8.1
			TC195	NAS NULL integrity with EIA0 is only used for emergency calls	Packet captures at the MME confirm that that the SECURITY MODE COMMAND message sent by the MME after successful UE authentication contains an algorithm different from EIA0 (except for emergency calls)	IMPLEMENTATION OPTIONS	MME	3GPP TS 33.116, cl. 4.2.2.3.3 3GPP TS 33.401, cl. 5.1.4.1
			TC201	eNB ensures confidentiality and integrity protection of control plane data	Packet captures confirm the use of IPsec on X2-C and S1-MME interfaces	IMPLEMENTATION OPTIONS	eNB	3GPP TS 33.216 4.2.2.1.1/4.2.2.1.2 3GPP TS 33.401, cl. 5.3/11 3GPP TS 33.501, cl. 5.4

Modified extract from one of the three data presentation sheets

2022 TIMELINE

5G Security Controls Matrix
powered by ENISA



Dec 2021

5G Matrix 2022 Pilot

5G Matrix Pilot workshop(s)

NRAs and MNOs

Preparation of the web tool user requirements

2023

Jan	Feb	Mar	Apr	May	June	July	Aug	Sep	Oct	Nov	Dec

2022 content additions

NRA consultation

2022 content additions

NRA and industry consultations

Publication of the Matrix (Excel)

LET’S JOIN OUR EFFORTS!

Specific questions about the Matrix?

How could the Matrix best assist you in your work?

How should the web tool be designed?

Which content additions should we focus on next?

5G Security Controls Matrix

powered by ENISA

THANK YOU!

ALL FEEDBACK, ADVICE, IDEAS, SUGGESTIONS WELCOME

☎ +30 693 651 3974

✉ slawomir.bryska@enisa.europa.eu

🌐 www.enisa.europe.eu