



# Industry Engagement Status by ITU-T SG17

Industry Engagement Workshop

March 2026

Arnaud Taddei – ITU-T SG17 Chair



# ITU-T Study Group 17 : Security ... and Trust

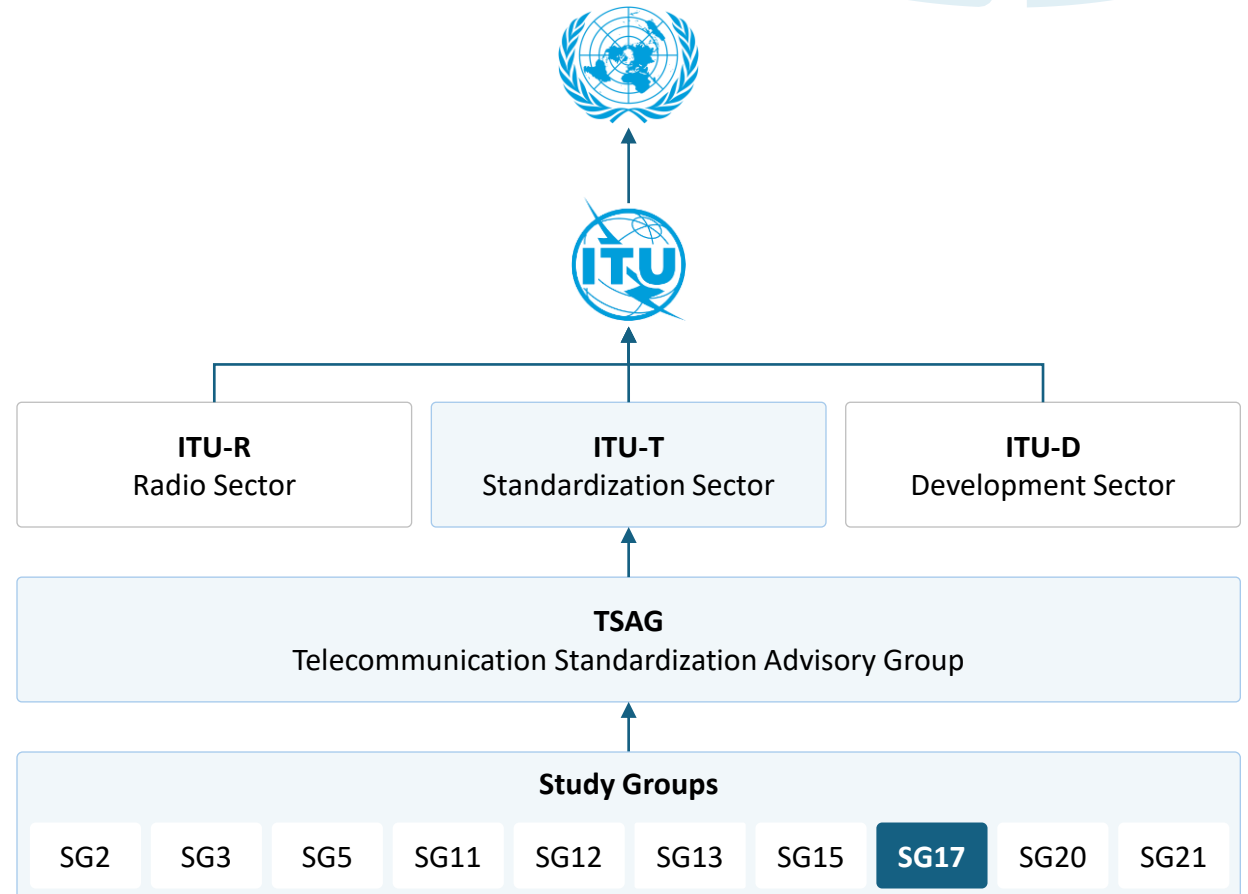
SG17 withing ITU-T context

Mandate Study Period 2025 - 2028



ITU-T Study Group 17 is responsible for developing international standards to enhance confidence, security and trust in the use of telecommunications/ICTs, in the context of an ever-growing attack surface and confronted with an unbalanced threat landscape.

In simple terms, SG17 is the Security and Trust group that delivers standards called Recommendations and non-normative texts such as Technical Reports, and many other deliverables



We are here



# ITU-T The biggest IPPPP!

International Public Private People Partnership

These come from two principal sources:

Consider the “skin in the game” model in place.

Member States want the Industry to leverage their collective world wide tax payer effort for making this world

opened, interoperable and AFFORDABLE

Industry membership contribution is small compared to the foundation that is sustained here ... since 160 years!!

The I...  
contri...  
spectrum and satellite coordination functions, develop technical standards and provide services to its members.  
ITU's total budgeted revenues in 2024 amount to around 165 million Swiss francs (CHF), or slightly above 190 million US dollars (USD) at current exchange rates.

Non-State Members - defined collectively as [Sector Members](#), [Associates and Academia](#) - contribute 9.9% of ITU's total budget in 2024. These contributors include private companies, other organizations, and academia, mainly paying through membership fees for different degrees of engagement.

# Current Structure

WP1

**Digital identity, Quantum based security, PKI and Fundamental security technologies**

Q10

Identity management and telebiometrics architecture and mechanisms

Q11

Generic technologies to support secure applications

Q15

Quantum-based security

WP2

**Security of IMT, IoT, metaverse and ITS/CAV**

Q2

Security architecture and network security

Q6

Security for telecommunication services, Internet of Things (IoT), digital twin, and metaverse

Q13

Intelligent transport system (ITS) and connected autonomous vehicle (CAV) security

WP3

**Cybersecurity and management, security strategy and coordination**

Q1

Security standardization strategy, incubation and coordination

Q3

Telecommunication information security management and security services

Q4

Cybersecurity and countering spam

WP4

**Security of AI, cloud computing services and applications**

Q7

Secure application services

Q8

Cloud computing and big data infrastructure security

Q14

Distributed ledger technology (DLT) security

SG17

# We come from somewhere

- An initiative path as SG17 Chair
- We inherit 3+ decades
- SG17 proved very resilient and survived COVID
- A very well-oiled machine
- A big family spirit
- A buoyant and very creative Study Group
  - Very innovative in many ways (e.g. DDP, A.1 table for NWI, first SG to run remotely in COVID, Incubation mechanism, First A.25 implementation, etc.)

# ... But we plateau ...

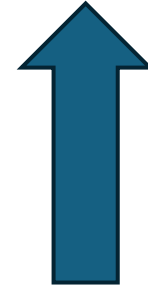
If we were to design an “SG17 performance global index”?

what would be the curve shape?

**SG17 is “plateauing” too**

the gains in specific areas of improvements ...

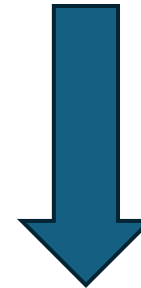
... are weighted by inhibitors



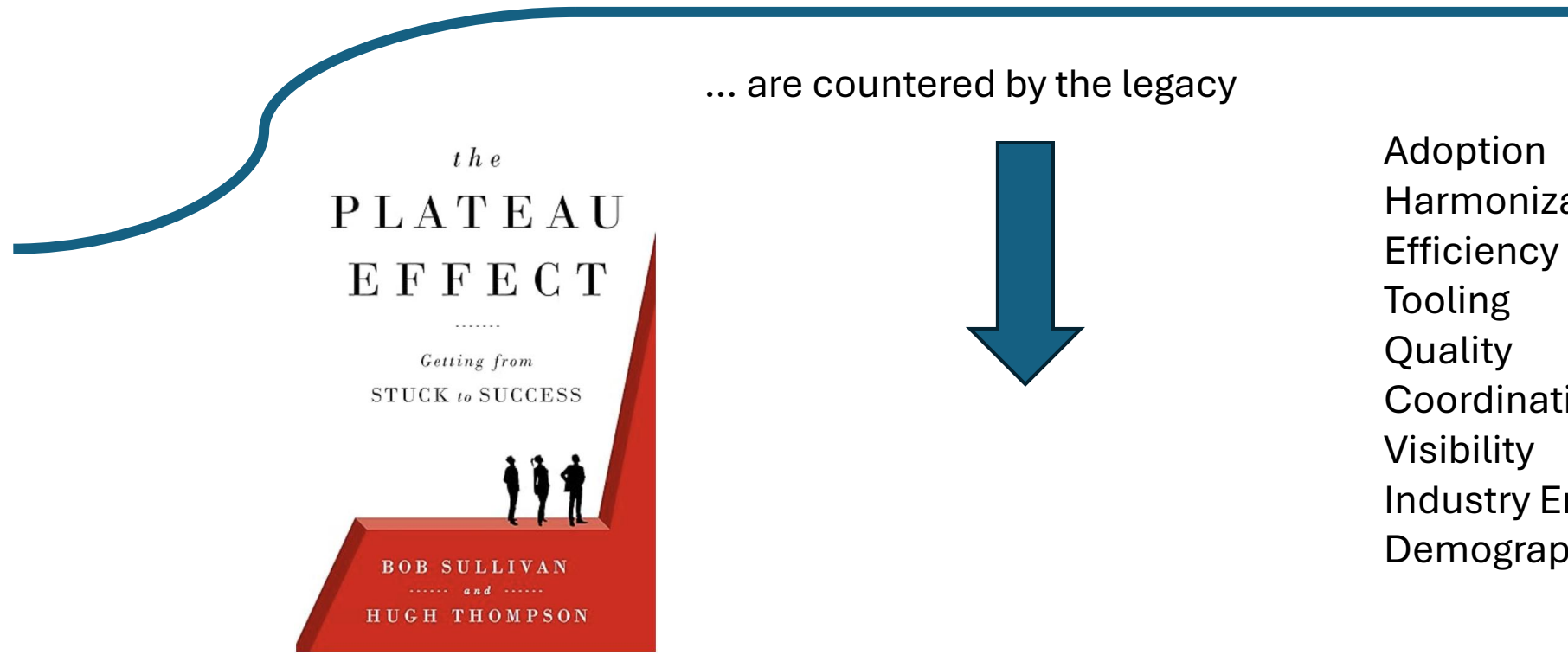
The generated gains ...

Structure  
Topics  
Volume growth  
Innovation

... are countered by the legacy



Adoption  
Harmonization  
Efficiency  
Tooling  
Quality  
Coordination  
Visibility  
Industry Engagement  
Demographics



# Some of SG17 key issues

## People at the heart of the problem and the solution

- If nothing special is done SG17 demographics will lead, long term, to:
  - A growing next generation big opportunity
  - A decrease of senior experts big risk
  - A stagnation of gender balance inacceptable
  - An under and decreasing representation of industry ➔ impacts relevance
  - An unbalanced geographic representation ➔ impacts global stds
- SG17 chair and vice chairs have a 4 – potential 8 years term
  - Normal case: need to find a new SG17 chair and leadership in 8 years
  - Worst case: in 4 years!
- It is absolutely CRITICAL to do everything possible to  
Address demographics now for the long term!

# Security is not in a good state

You may not like it, but Security is in a broken state!

**A growing cacophony**



Too many actors are literally 'paid' to invent new words every 'N' years

We are missing an equivalent of the 'OSI Model for Networks (the 7 layers)' in the field of Security

**Worst, we are losing the war**



We are told: **\$6T** of harm in 2021 → **\$10T** in 2025 → **\$20T** in 2035? Or in 2030?

Even if the numbers are wrong: the level is way to high and we are not impacting 'their' growth!

Innovation, e.g. AI, accelerates 'them', IoT attack surface explosion, etc.

How many catastrophes and drama do we need?

**That is a KEY Question we should address.**

**More complications**



**Expect more (fragmented) regulations**



With good, bad and ugly consequences

**3 body problems**



Privacy vs Security vs Safety is a touch challenge

**Time Dimension**



Too many things to resolve in the 10+ coming years

**Resources Dimension**



Missing people, energy, money to fix it all in the next 10+ years

# Few things about the chair

Drivers

- \$10T of harm is intolerable. How to hyperscale security?
- Standardization is NOT established for the security market. How to fix it?
- Too many unbalanced parameters for the next 10 years. How to heal?

Doctrine

Conservatist

Cautious Reformist

Reformist

Time mangement behavior

Active Procrastinator

Planner

I like Performance,  
HyperScalability,  
Impact and sane  
Competition!

Hate surprises

Proactive

Reactive

How success looks like

- One Recommendation recognized by one major jurisdiction (eg EU)
- Security standardization better recognized by the market
- SG17 conditions improved and
  - industry is joining back
  - Talents join SG17 and we are an excellence center (e.g. models)

Not an empire  
builder

# The SG17 modernization story is simple

*“This all about giving SG17 relevance back to the market, the industry and the regulators, for the next generation and as inclusive as possible.*

*All the proposals in this presentation are driven by this primary objective”*

Arnaud Taddei – March 2024

# WTSA24: The best ever ITU assembly

Outputs ([Draft Proceedings](#)) See [TSB Circular 1](#)

## Resolutions

- Many new Resolutions with instructions for SG17: Res. 101 (AI), Res. 103 (DPI), Res. 104 (Vehicular), etc.
- Engagement<sup>1</sup> which will shape SG17
  - 2 New Resolutions: Res. 107 (Next Generation) and Res. 108 (Strategic Planning)
  - Res. 68 (Industry), Res. 55 (Gender), Res. 22 (TSAG), Res. 74 (Sector Members in Developing Countries), Modified
  - New WTSA Actions through WTSA24 report
- Cyber
  - Res 50, 52, 58 Modified
  - New WTSA Actions through WTSA24 report to SG17: COM4/5 (digital identities)<sup>2</sup>, COM4/8 (PQC)
  - A brilliant Cyber ad-hoc sessions chair!

## A new chair and vice chairs

- Already a difficult set of Resolution 2 ad-hoc sessions<sup>3</sup>
- A good agreement with SG21 chair and fixes to accommodate other SGs perception
- A robust ask to TSB at the training regarding TSB Strategy
- Inviting the chair of the IETF was critical

1) Part of WG3B led by M. Arnaud Taddei

2) mindful of the new Resolution on Digital Public Infrastructure (DPI) and the TSB Circular 6 of OpenWallet Forum

3) former chair, new chair, and SG17 delegates in action!

# A program with five pillars to execute the Vision

Extract modernisation objectives for SG17

Improve Efficiency	Improve Quality	Improve Coordination	Improve Visibility	Attract Industry
<p>Leadership Structure Working Parties reinforced SG17 Meetings Workshops Others Tooling (Github)</p>	<p>Competence Center</p> <ul style="list-style-type: none"> <li>• Establish a Comp. Center</li> <li>• Domain(s) Knowledge</li> <li>• New and Emerging</li> <li>• e.g. Models</li> </ul> <p>New Work Items</p> <ul style="list-style-type: none"> <li>• Market representation</li> <li>• Global</li> </ul> <p>Split issues in 3 phases:</p> <ul style="list-style-type: none"> <li>• Pre New Work Item est.</li> <li>• Work Item development</li> <li>• TAP/AAP phase</li> </ul> <p>Peer review</p>	<p>Rethink coordination:</p> <ul style="list-style-type: none"> <li>• what do we trade?</li> </ul> <p>Internally:</p> <ul style="list-style-type: none"> <li>• SG17</li> <li>• ITU-T</li> <li>• ITU</li> </ul> <p>Externally:</p> <ul style="list-style-type: none"> <li>• Other SDOs</li> <li>• and fora</li> </ul>	<p>Inclusivity and Diversity</p> <p>Internally</p> <ul style="list-style-type: none"> <li>• SG17</li> <li>• ITU-T</li> <li>• ITU</li> </ul> <p>Externally</p> <ul style="list-style-type: none"> <li>• Other SDOs</li> <li>• Regulators (esp. EU)</li> <li>• Industry with specifics</li> <li>• Academia with specifics</li> <li>• Member states with spec.</li> <li>• Social Networks</li> </ul> <p>Revisit Communication</p>	<p>Specific campaign</p> <p>Focused/coord. approach:</p> <ul style="list-style-type: none"> <li>• TSB</li> <li>• SG17 leadership</li> <li>• SG17 Rapporteurship</li> <li>• Affiliations</li> </ul>

# A comprehensive program

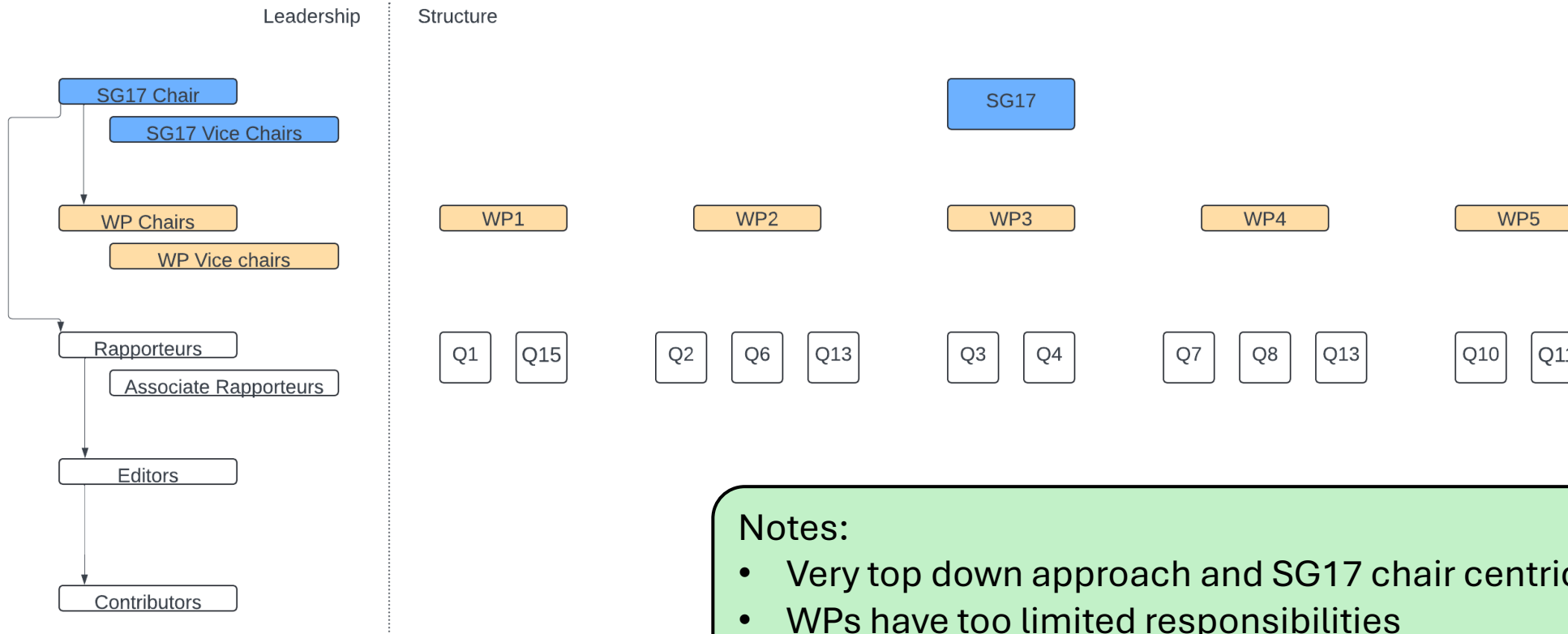
## 2 Correspondence Groups

- correspondence group on restructuring and modernization (CG-RES-MODERN)
- a first methodic strategy for AI Security with CG-AISEC-STRAT
- A high cadence peaked at 3 meetings a week for 3 months across a 100 participants
- Dozens of TDs and Contributions
- Now moved on an on premise GitLab (Experimental) hosted by ITU-T
- 130 issues, huge efficiency win (and this is just the beginning!)

The image displays two overlapping screenshots of the GitLab web interface. The left screenshot shows the 'Study Group 17' page, which includes a sidebar with navigation options like 'Pinned', 'Issues' (130), and 'Merge requests' (0). The main content area lists 'Subgroups and projects' such as 'AI security standardization roadmap', 'Closed Management Team', 'SG17 Modernization', and 'SG17 Work Items'. The right screenshot shows the 'Issue Boards' for 'SG17 Modernization', featuring a Kanban-style view with columns for different packages (PKG1 to PKG7) and tasks (T1.5.1 to T1.8.3). Each task card includes a title, priority (e.g., (SP1) Efficiency), and a due date.

# What's wrong with how we develop content? 3/3

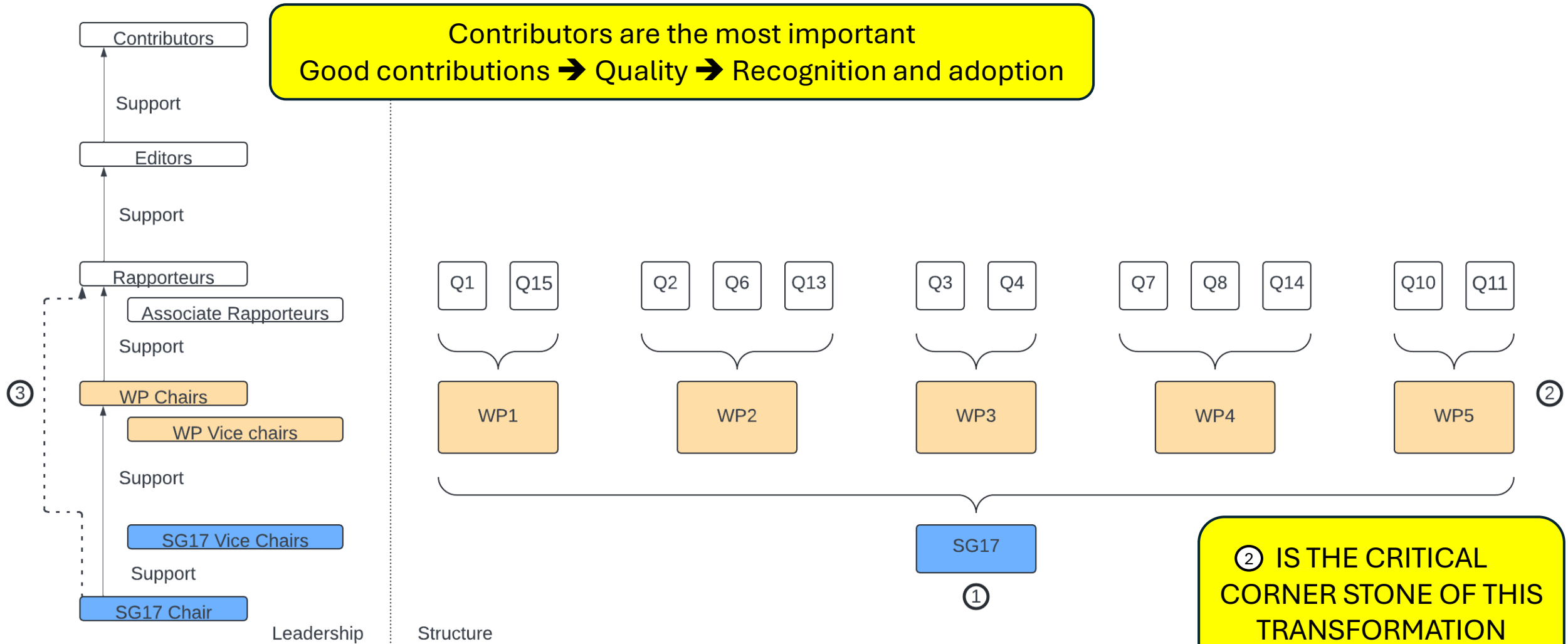
## Need to ask the hard questions: A culture issue



### Notes:

- Very top down approach and SG17 chair centric
- WPs have too limited responsibilities
- We ONLY Reward experts with leadership positions!
- We have no way to reward experts with experts titles
- Contributors names are not publicly available
- We reward bad behavior

# The change starts with organization culture



Notes:

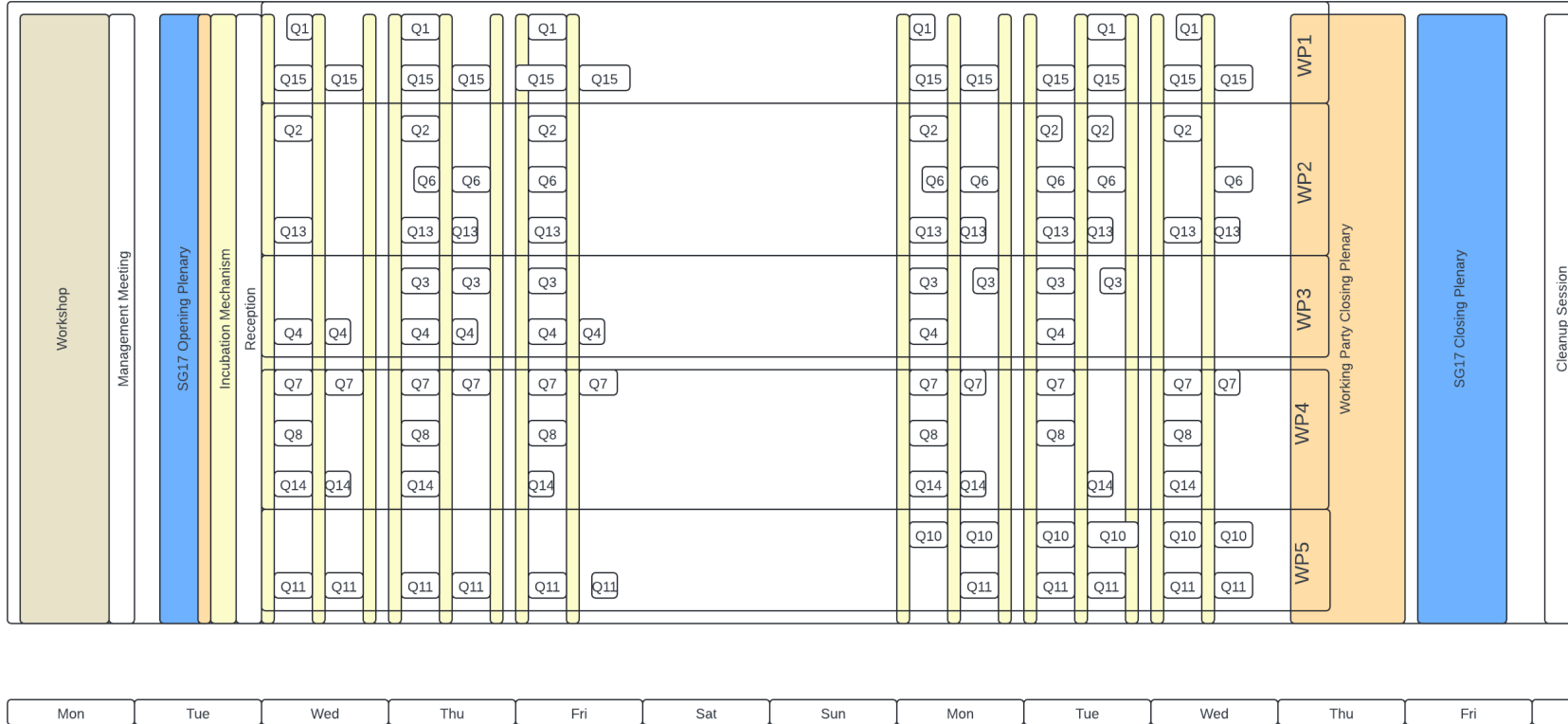
- ① The SG17 chair is doing the best "top down" job when required
  - But the SG17 Chair hopes that most of its time will be a 'sparring partner job' → **Reverse Pyramid**
- ② Working Parties have more power and support their Questions and frame any activity, in a more cohesive manner
- ③ The chair decreases too many direct access to Rapporteurs and, with SG17 Vice Chairs, empowers Working Party Chairs and Vice Chairs

# Working Party Level – Chairs – Selection Criteria

Criteria	Description	Rationale
Skills and Competencies	Working Party Chairs demonstrate standardization leadership skills and competencies	<ul style="list-style-type: none"> <li>- Basic requirement from Resolution 1</li> <li>- Skills are transferable but competencies are not (attached to each individual)</li> <li>- Competencies are the essential leadership aspect required because of the modernisation of SG17</li> <li>- Skills can be transferred to the new chairs</li> </ul>
Industry	Working Party Chairs come from the industry	<ul style="list-style-type: none"> <li>- Deviation from Resolution 1</li> <li>- Biggest problem to fix in SG17 (lack of industry participation)</li> <li>- SG17 chair alignment to Industry Engagement work at TSAG</li> <li>- First industry onboarding experiences already support this criteria</li> <li>- SG17 chair alignment to WTSA24 (WG3B) Res. 68</li> </ul>
Next Generation	Working Party Chairs come from the Next Generation	<ul style="list-style-type: none"> <li>- SG17 chair himself is from the Next Generation</li> <li>- SG17 demographics cause two problems: decrease of senior members, increase of Next Generation</li> <li>- SG17 chair alignment to WTSA24 (WG3B) and New Resolution 107</li> </ul>
Gender Balance	Working Party Chairs are gender balanced (2 men, 2 women)	<ul style="list-style-type: none"> <li>- Good women representativity in SG17</li> <li>- SG17 chair wants to improve conditions to improve the experience for all and in particular for women</li> <li>- SG17 chair alignment to WTSA24 (WG3B) and updated Resolution 55</li> </ul>
Geographic Diversity	Improve geographic diversity	<ul style="list-style-type: none"> <li>- There are several unbalanced geographic issues</li> <li>- Only four positions so needed to both anchor existing representation vs giving positive signal for other regions Res 74</li> </ul>

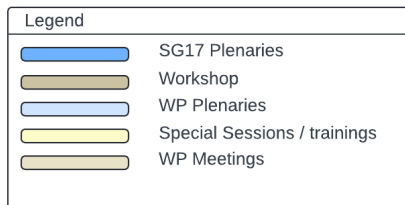
# What's wrong with our SG17 meetings? 6/6

Need to ask the hard questions : Are we using the time correctly?



Data from SG17 February 2024 meeting

- 56% usage of time slots by Questions!
- Some time slots used for a short amount of time (20' – 30'!)
- Some rooms nearly empty!



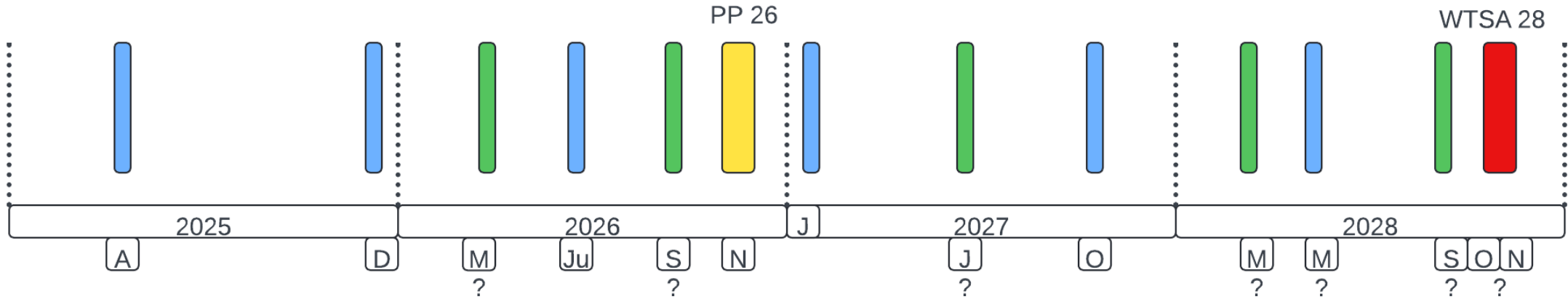
NOTES:



- Total number of blocks for questions: 24x12 = 288
- Questions total fill up rate: 162
- Questions blocks utilisation: 56%
- Total unused time: 126x1.15h = 6 days (parallels) --> more than half day could be saved immediately

# How does it translate? Efficiency

Before	Now
Only SG17 plenary meetings: workshop + work on content + decisions	Separation between to redistribute the energy SG17 plenary meetings: focus on decisions and efficiency SG17 content weeks: workshops + RGMs + WP meetings focus on quality but contributes to more efficiency in plenaries
2 SG17 plenary meetings a year	3 SG17 meetings a year: 1 plenary + 2 content weeks (when there are assemblies) or 2 plenaries and 1 content week
10 days long plenaries	8 days long in April 25, 7 days long in December 25, back to 8 days long in June 26, new attempt for 7 days long in January 2027
LS/o processed in Questions, Closing WP and Closing SG17 meetings	LS/o processed more continuously and with dedicated SG17 plenary sessions in SG17 plenary meetings: gained 8 hours of WP and SG17 closing at the first attempt
12 Questions in parallel but 56% sessions occupation	Reduce step by step the parallelism led to 95% sessions occupation in December

# SG17 Meetings and Content Weeks Cadence



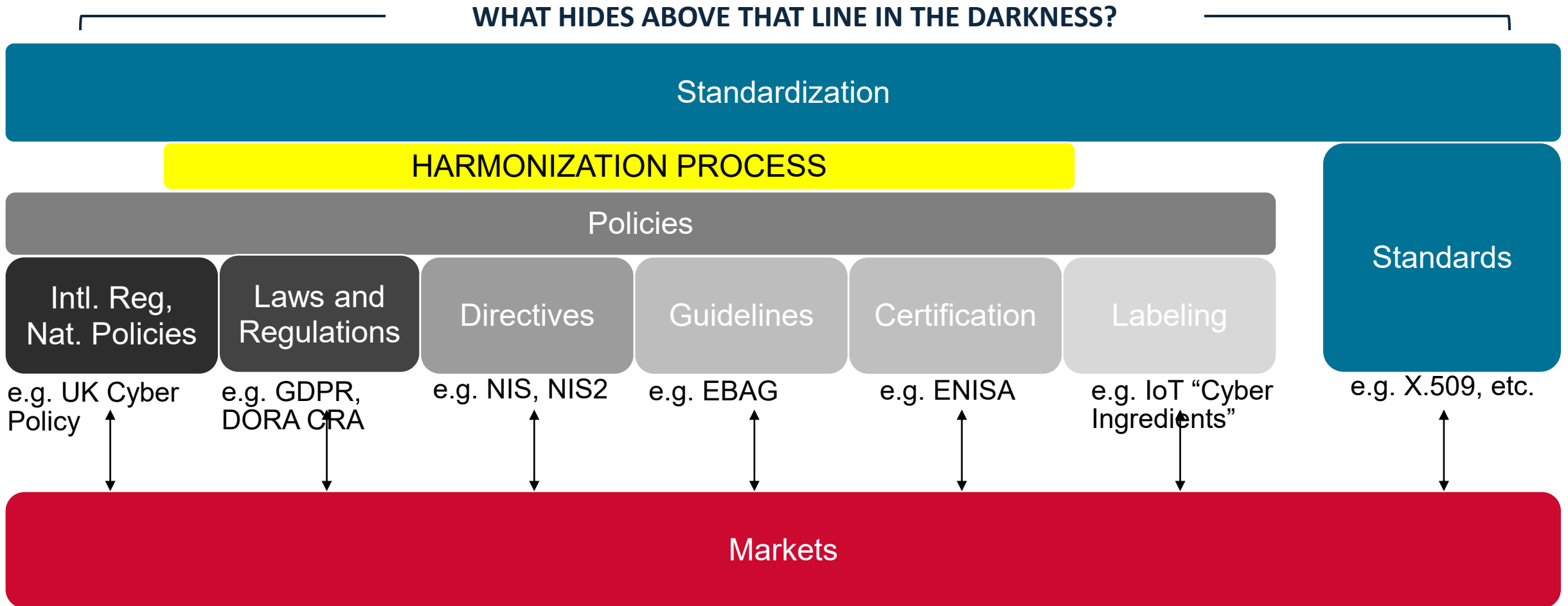
Legend	
	SG17 Meeting
	SG17 Content Week

## Notes:

- 6 SG17 Meetings
- 5 SG17 Content Weeks
- SG17 meetings fixed with TSB until 2027 – Need to wait for Council decision to fix SG17 meeting in 2028

# Why standardization matters

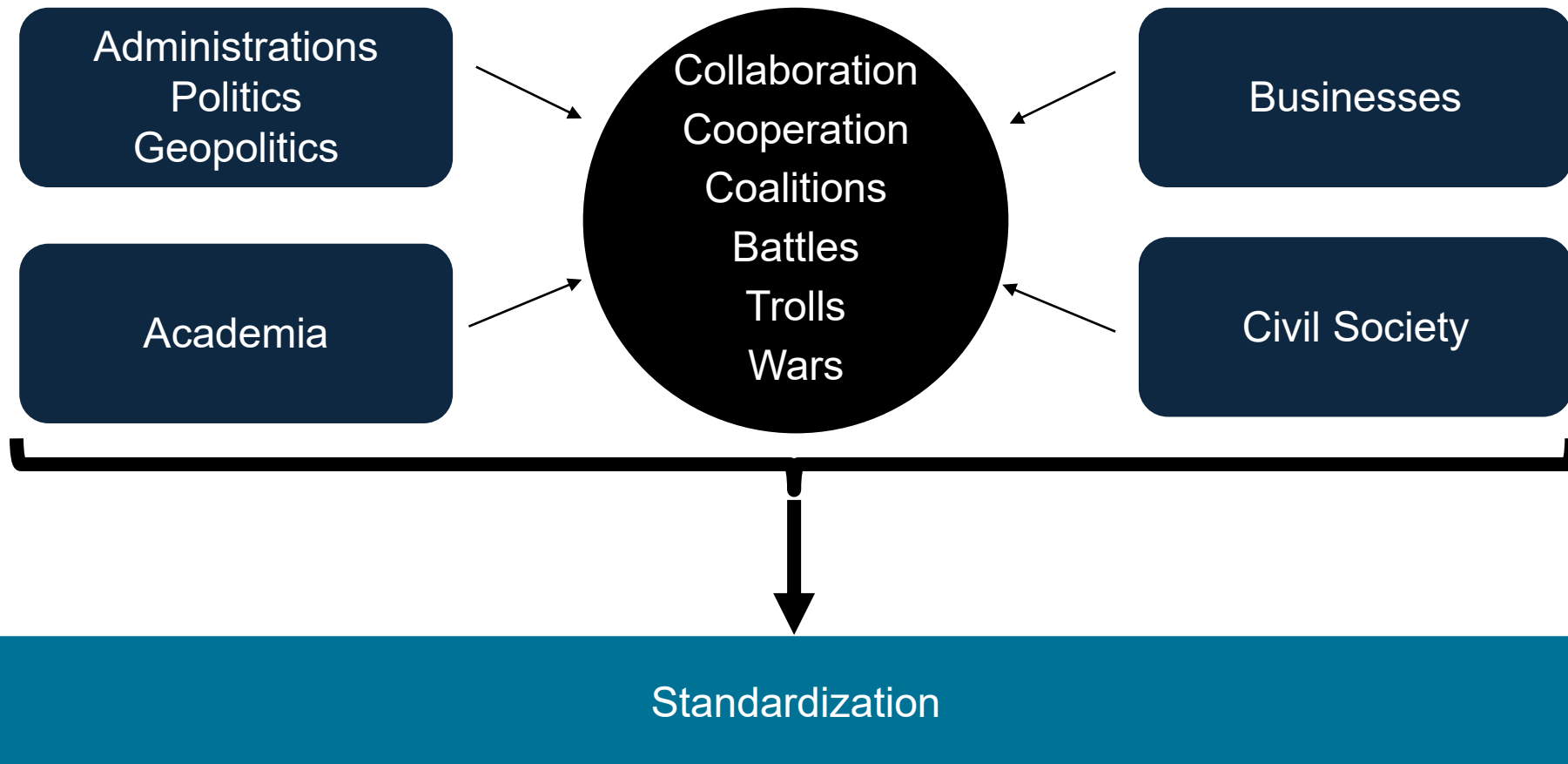
Unlike eg. Mobile networks, for security, an unrecognized but growing mechanism that shapes markets



# “The dark matter” behind Standardization

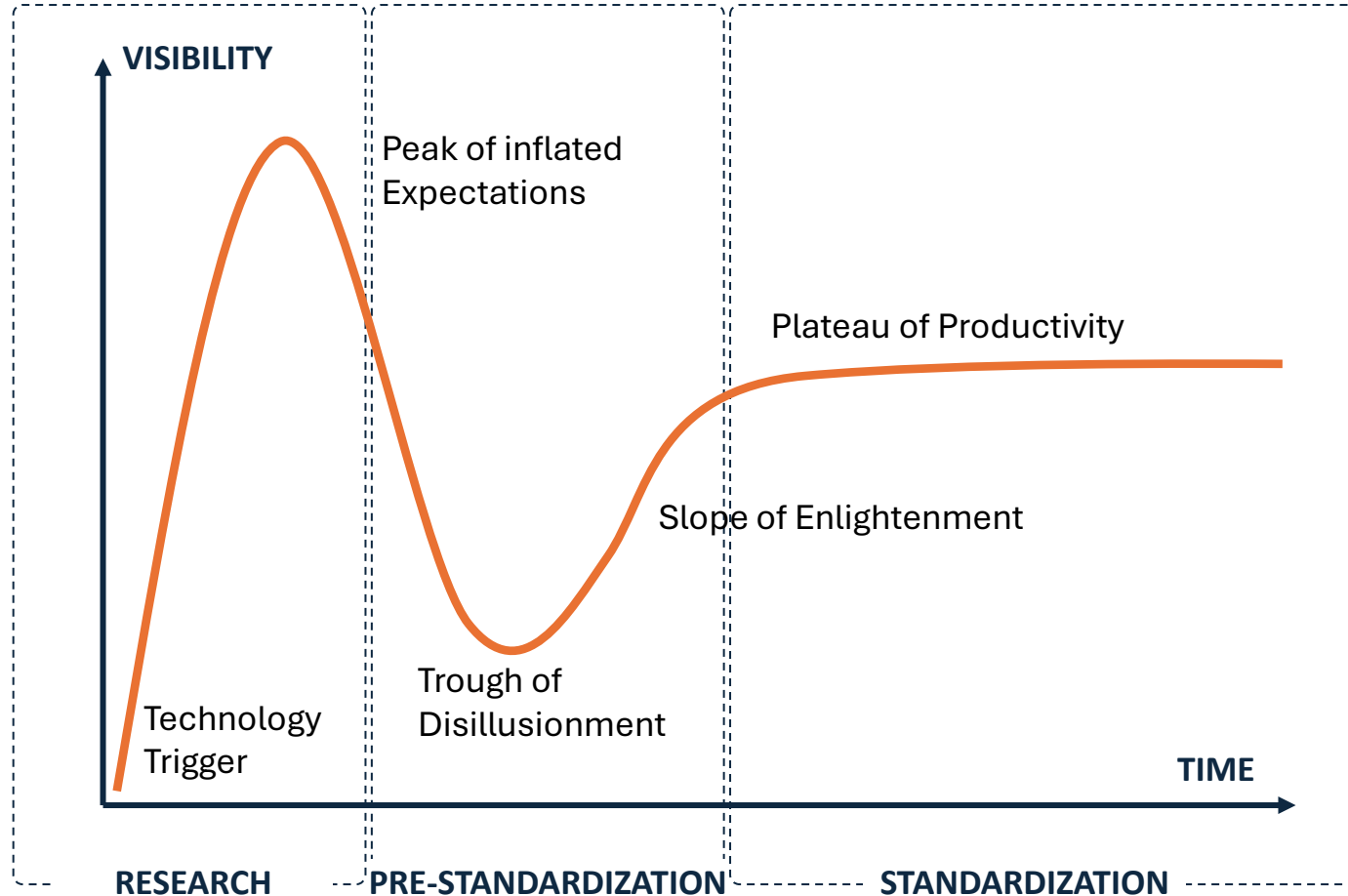
The key Unique Selling Point of the ITU and SG17 in particular!

The good, the bad and the ugly too ... No risk, no benefit



# When to standardize?

The billions dollar question



**Standardization happens to remove frictions in the market, and its timing is essential.**



Too early risk to inhibit the development of the market,



Too late solutions are too well established.



It happens when there are too many solutions blossoming on the market and it is time to pick a few or one

# SG17 2<sup>nd</sup> Plenary (3-11 December 2025) Exec Summary

## An historic milestones

SG17 KPIs	Results
Participants	New Record 400+ from 57 Countries
Contributions	New Record 231
Total Work Items	New Record 191
New Work Items	New Record 65
Quality jump	Rebalancing NWI vs WI and NWI established at 85%
Restructuring	Creation of Question 16 AI Security, Question 3+Question 10 Merge Digital Identity + Cyber Defence Centers, Question 7 Application Security Amended for AI 4 Workshops (3 on AI, 1 on PQC and X.509), 2 Correspondence Groups, 3 JCAs, 1 CQR, All planning until 2028, ...
Topics	AI, gen AI, Agentic AI, Digital Identity, Trust, 5G/6G, PQC, QKD, Y2K38, Digital Emblems, Child Online Protection, IoT Security, Intelligent Transport Systems, Cyber Defense Centers + CSIRT, Cyber Assurance

# Who is attending SG17

Traditionally, roughly

- 40% Regulators
- 40% Associate and Sector Members
- 15% Academia
- 5% Civil Society
  
- CKJ Dominated
- With strong participation from UK, US, Canada
- Little to no presence from EU or EU member states
- Very little presence from Western security industry
- Strong presence from developing countries regulators

The key discovery to establish standardization in the security domain: Convince CUSTOMERS to join! (learning from IEWS #1)

Finally other vendors and competitors

Since 10 months due to vigorous modernization program

- Net new or now, active members
  - Thales
  - Cognizant
  - Google
  - Microsoft
  - Vodafone Group
  - Zscaler
  - Amazon
  - Metomic
  - TNO
  - Statestreet
  - FIRST
- In the pipeline confirmed
  - Salesforce
  - Servicenow
  - MBCOM
  - Logically
  - Schneider Electric
- In the pipeline considering
  - Another 25 names all on Western industries including prominent stakeholders, OI DF, Sidi Hub, etc.
  - A significant number of top tier financial institutions
    - Including initiatives starting at FS-ISAC to join standardization

The importance of other for a (learning from IEWS #1)

# SG17 Industry Engagement workshops

First experimental Industry Engagement Workshop in Washington DC in September 25

- 7-10 people supposed to join
- 40 turned up
- If I could have anticipated we would have ended 65!
- A MASSIVE success
  - Format worked
  - Focus on Why and What is in for me
  - Break the ice between the stakeholders (US and UK administration, Industry, existing and new comers, SG17 leadership)
  - Identification of successes, issues and gaps (eg Finance sector not coming! Value proposition biased for vendors and not for customers)

New request by a tier 1 European country for a second on in 27 for 90 people

Working on next demands for 28 (Administrations need a lot of elapsed time)

# Visibility

First article on Agentic AI and Digital Identiy

<https://www.itu.int/hub/2026/01/why-standards-are-key-to-agentic-ai-security-and-digital-ids/>

HUGE IMPACT! Up to highest levels of prominent administrations

Ramping up our communication execution! This is that simple!

Designated Promotion Officer: Ms Honey Makola (SG17 VC)



Arnaud Taddei · You

Global Security Strategist, Enterprise Security Group at Broadcom | ITU...

1mo · 🌐

I am very proud and pleased to present our first SG17 press release

"Why standards are key to agentic AI security and digital IDs"

<https://lnkd.in/eAuJwFwG>

Check this press release and its youtube. Feedback welcome.

The level of friction in this field is probably evaporating billion of dollars and interoperable standards are bitterly needed.

SG17 is proud to share that we are taking the leadership in this area and you are all cordially invited to the 3 coming, connected workshops below, opened to everyone and free.

The rally to SG17 is unprecedented with an acceleration of membership from a broad and varied industry, member states, academia and civil society.

Now is the opportunity to resolve for big problems and have an impact together.

30-31st of March SG17 Workshop in Geneva during the 1st Content Week Trustable and Interoperable Digital Identities for Human and Agentic AI

(provisional) 3rd of June SG17 Workshop in Geneva during 5th SG17 Plenary Meeting

Globally interoperable digital identity

(provisional) 10th of July SG17 Workshop in Geneva during AI for Good Designing the Trust Management for Agentic AI



**Why standards are key to agentic AI security and digital IDs - ITU**

itu.int

Kseniia Fontaine and 87 others

2 comments · 8 reposts

# ITU-T SG17 Status on Agentic AI Security and Trust

## A strategy, A new structure, First work items, A roadmap, A schedule

### In general a LOT of work since December 2024 at high cadence

- ITU-T SG17 grew to 400 participants and 57 member states as per strong modernization program
- One new member per month mostly western industry (Thales, Cognizant, Google, Vodafone, etc.)
- First workshop Challenging the status quo on AI Security 11th of July 2025 ([LS 2077](#))
- AI Strategy available to IETF ([LS 2106](#))

Leads to

### Restructuring (to be fully approved beginning April)

- Creation of new Question 16 for AI Security including Agentic AI with a carve out for no overlap with IETF!
- Merge of Question 3 and Question for Agentic AI Digital Identity
- Amendment of Question 7 for Agentic AI

Leads to

### Out of 40 work items on AI security 7 are related to Agentic AI (+20 in draft!)

- [X.LLMCC](#) Guidelines for large language model data security based on confidential computing, already sent to IETF per [liaison 2108](#)
- [X.S-AIA](#) Security requirements and guidelines for Artificial Intelligence agent
- [XSTR.sem-AIA](#) Security evaluation methods for Artificial Intelligence agent
- [X.sr-taimas](#) Security requirements for terminal-based artificial intelligence multi-agent system
- [X.dpidm-aAI](#) Terminology and design guidelines for Agentic AI identity management
- [XSTR.gidi](#) Globally interoperable digital identity (including humans/enterprise/non-humans i.e. Agentic AI) **Even the European Union contributes!**
- [XSTR.ltf-AAI](#) Landscape of trust framework for agentic AI

Leads to

New Q10 work items

### A specific scheduled roadmap through Workshops opened to everyone and SG17 meetings

- **1st Workshop** 30-31st of March - [ITU Workshop on “Trustable and Interoperable Digital Identities for Human and Agentic AI”](#)
  - First SG17 Content Week 30th of March - 2nd of April
- **2nd Workshop** 2nd of June - Workshop on globally interoperable digital identity
  - Fifth SG17 Plenary 1-10th of June
- **3rd Workshop** 10th of July - Designing Trust Management for Agentic AI
  - AI for Good 6-10th of July

Supports / is supported by

Leads to

Leads to

# SG17 AI Security Workshop

AI For Good: 11<sup>th</sup> of July 2025



SG17-TD138/PLEN  
STUDY GROUP 17  
Original: English

Question(s): ALL/17 TD Geneva, 3-11 December 2025

Source: Chair SG17

Title: Report and presentations of AI Security Workshop at AI for Good Global Summit 2025

Contact: Arnaud Taddei Email: [arnaud.taddei@broadcom.com](mailto:arnaud.taddei@broadcom.com)  
Broadcom Europe

Abstract: This document contains the report and presentations of the AI Security Workshop "Challenging the status quo of AI security" organized by ITU-T SG17 on 11 July 2025 at AI for Good Global Summit 2025

Please see below.

## AI Security Workshop Report "Challenging the status quo of AI security" at AI for Good Global Summit 2025

1. Date and Venue .....	1
2. Opening .....	1
3. Keynote: Framing Agentic AI and Identity with a Strategic Lens .....	2
3.1. Introduction .....	2
3.2. Key Takeaways .....	2
4. Session 1: Agentic AI Security .....	2
4.1. Introduction .....	3
4.2. Main Discussion .....	3
4.3. Key Takeaways .....	7

unique on the trust model

- ✓ Organizations need to establish an internal committee for AI within their "Enterprise AI Governance" scope

### 7. Closing

SG17 Chair, Mr Arnaud Taddei, closed the workshop at 12:30 after he thanked the questions from enthusiastic audience participated until the end in a packed room.

His main observation echoed the keynote speaker that this workshop provided the contours of standardization work and that the effort is at the level of what the OSI model for Network was 40 years ago.

This time this is about an OSI model for AI or Agentic AI. The metaphor works to a certain degree: need for a meta model (based on mental models), a communication protocol, a security model, an identity model, etc.

But it requires too some new considerations that were not there 40 years ago:

A full trust model and its Agentic AI trust control plane where:

- Trust includes a number of design characteristics: security, privacy, safety, resiliency, etc.
- Human beings are involved with e.g. a stop button or a let-go button and other scenarios,
- The trust control plane can specify trust objectives or multi-objectives to the multi-agentic AI systems it controls,

A different approach to the payload of multi-agentic AI communication itself given the significant challenges posed by e.g. hallucination attacks from a business standpoint up to, in some cases, an existential danger to society. Enterprise governance is a good approach in scope to technical standardization that should provide the requirements, use cases and new solutions to address this issue.

SG17 Chair articulated briefly the next steps after this workshop:

- immediately after the workshop, Mr Soumil Yu, Mr Babak Hodjat, Ms Debora Comparin and Ms Xiaofang Yang will be in Central Stage at the closing plenary of AI for Good,
- a report (this report) will be produced as input to SG17 AI Security Strategy and SG17 Restructuring,
- a communiqué will be prepared in September 2025,
- New Work Items will likely be offered as Contributions to the 2<sup>nd</sup> SG17 meeting in 3-11 December 2025 in Geneva,
- A dedicated workshop on Digital Identity will be organized in Spring 2026 including for Agentic AI
- A second AI Security Workshop will be proposed for AI for Good 2026.

SG17 Chair, thanked all the contributions and sharing of their leading expertise from the panelists and moderators, and the support from ITU-TSB secretary team Ms Xiaoya Yang, Ms Gillian Makamara, and Mr Youssef Bayouh in the preparation and organization of this workshop.

This time this is about an OSI model for AI or agentic AI.

The metaphor works to a certain degree: need for a meta model (based on mental models), a communication protocol, a security model, an identity model, etc.

But it requires too some new considerations that were not there 40 years ago:

A full trust model and its Agentic AI trust control plane

...

# Digital Identity and Trust Management Framework

The real elephant hidden in the room!

Agentic AI

Currently no interoperable digital identity and trust framework

	Human Digital Identity	Enterprises	Non Human Digital Identity
<b>Protocols / Schema</b>	On track	<ul style="list-style-type: none"> <li>• Partial</li> <li>• LEI for FI vertical, mdoc/mDL for driving license use case</li> </ul>	<ul style="list-style-type: none"> <li>• Emerging</li> <li>• de-facto protocols e.g., MCP, A2A</li> </ul>
<b>Trust Management</b>	<ul style="list-style-type: none"> <li>• Country-led e.g., AAMVA, Austroads “VICAL” for driving-license use case</li> <li>• Partial for Regional e.g., eIDAS2</li> <li>• Gap for Global</li> </ul>	<ul style="list-style-type: none"> <li>• Partial</li> <li>• LEI for FI vertical</li> </ul>	Gap
<b>Policy / Trust Framework</b>	<ul style="list-style-type: none"> <li>• Country-led Partial for Regional</li> <li>• Gap for Global</li> </ul>	<ul style="list-style-type: none"> <li>• Partial</li> <li>• LEI for FI vertical</li> </ul>	<ul style="list-style-type: none"> <li>• Emerging (select country, regional laws)</li> </ul>

Source:

ITU-T SG17

[XSTR.gidi: Globally Interoperable Digital Identity \(including Humans / Enterprise / Non-Humans i.e. Agentic AI\)](#)

# How does this translate into Standardization space

Example of SG17! A Weekly cadence to win the Agentic AI pole position ...



# Conclusions

- 2022 was a disaster for Industry Engagement (Res 68 at WTSA20 and loss of the new resolution at PP26)
- But the WTSA Action gave a MASSIVE win at TSAG and led to a brilliant Action Plan
- First Industry Engagement workshop was a recognized high success
- WTSA24 changed the game for engagement
- SG17 modernization is beyond trajectory (far beyond)
- This starts to be recognized by the industry (and on the West)
- Agentic AI leadership is accelerating industry engagement
- It is deeper than that: this is about to establish standardization in the field of security

Thank you