

The Potential Cyber & Network Security Issues of PSTN Closure



Andy Valdar

FITCE UK, ITP

Honorary Professor at University College London

Agenda

1. Scene setting
2. Closure of PSTN
3. Issues with an all-IP network
4. Opening of operators' networks
5. Conclusions

1. Scene Setting

Scene Setting

This is an age of rapid change in the telecommunications world –

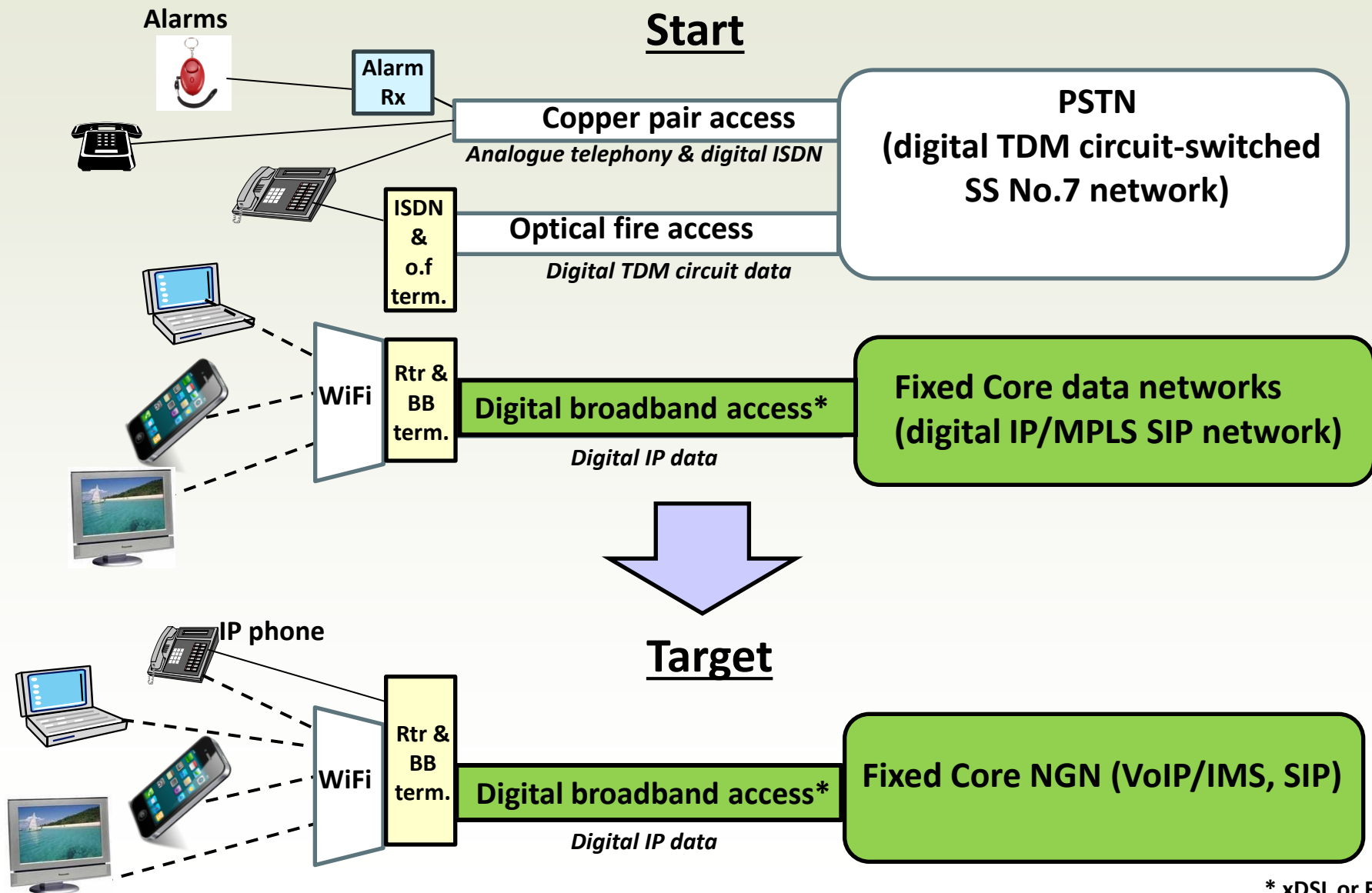
1. Rapid increase in customer demand for broadband capacity
2. Rollout of fixed line optical fibre broadband to domestic and business customers
3. Digital transformation by business customers
4. Rollout of 5G mobile
5. Increasing availability of LEO broadband satellite services
6. Huge increase in use of cloud by business customers as well as network operators
7. Introduction of virtualisation in networks, NFV
8. Introduction of Open Network APIs

The most significant digital transformation by Network Operators is the replacement of the TDM digital voice switching by an all-IP digital common services network

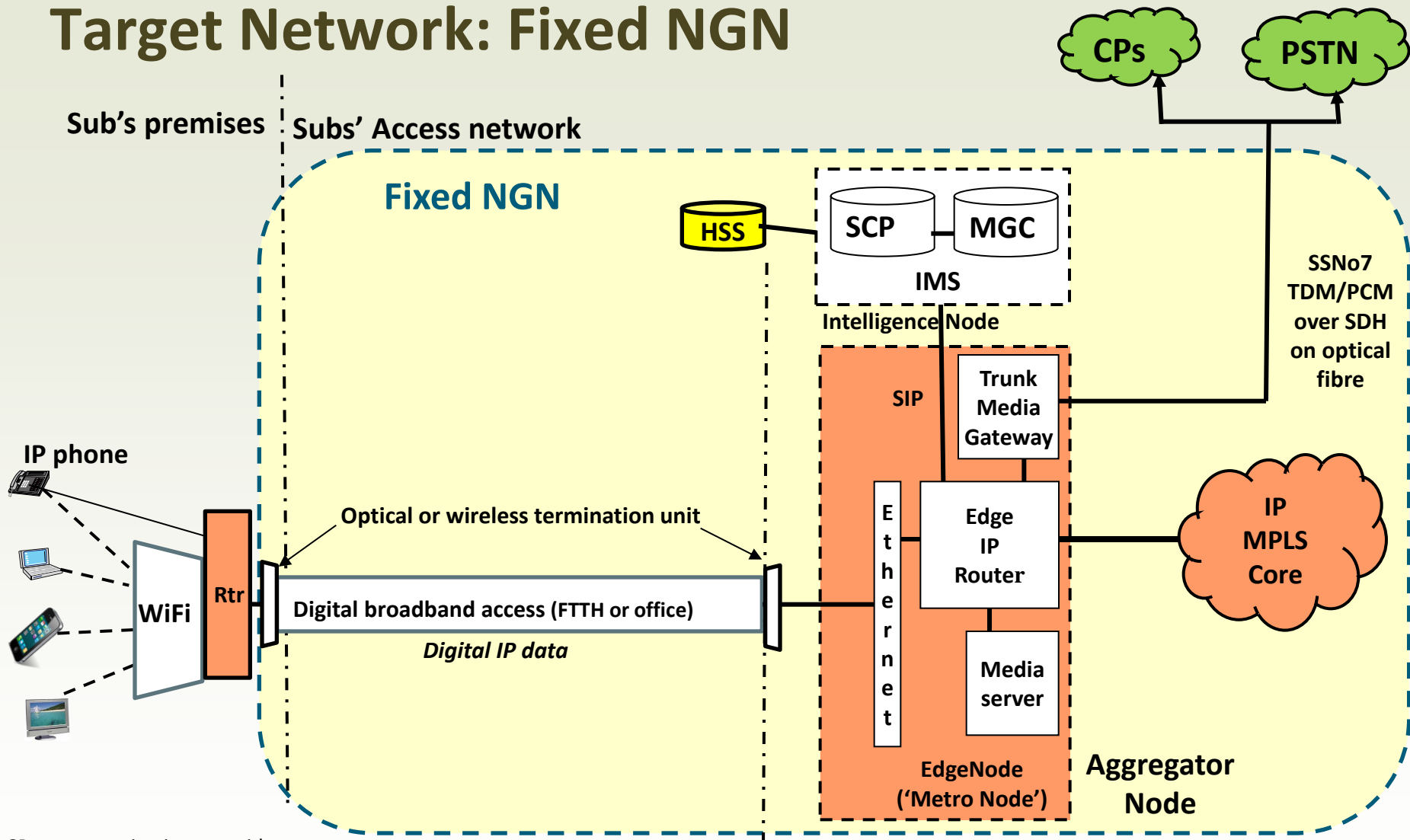
.....i.e. PSTN closure

2. Closure of PSTN

Closure of PSTN & Move to All-IP Network (NGN)



Target Network: Fixed NGN



CP = communications provider
HSS = home subscriber server
IMS = IP multi-media server
MG = media gateway
MGC = media gateway controller
SCP = service control point

Issues with Closure of PSTN

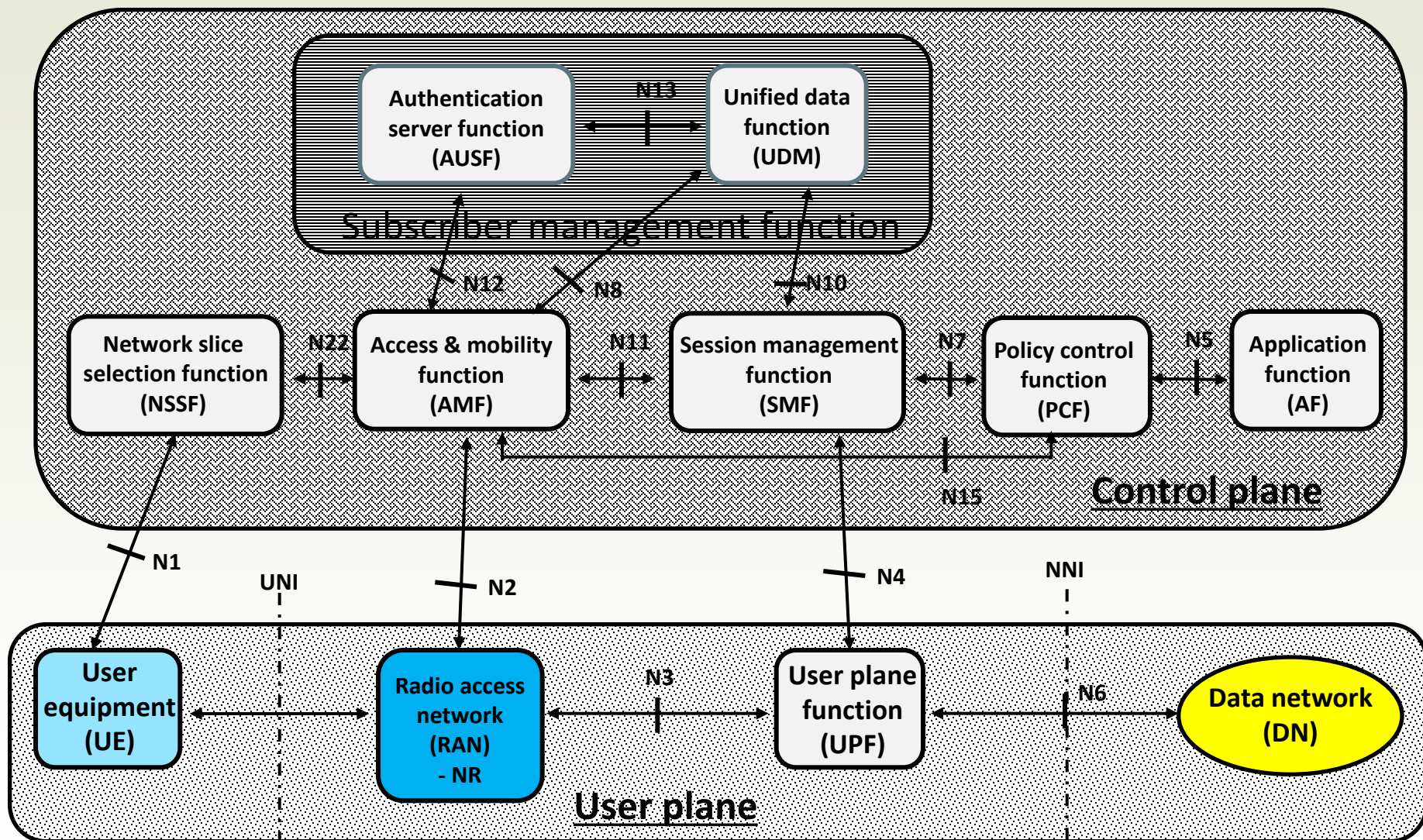
1. Withdrawal of network powering of sub's apparatus
 - *Need for no-break supply back up*
 - *Reliance on cellular mobile back-up to telephone (and broadband)*
2. Withdrawal of copper local line means loss of metallic path
 - *Non-voice customer systems not supported*
3. Lack of circuit emulation in all-IP network means cannot support alarms – house security alarms, vulnerable people fall alarms, etc.
 - *Need for new IP-based replacements [POTENTIAL IOT SECURITY VULNERABILITY]*



Potential Security Issues with Shifting PSTN Services to a Common Services All-IP Platform

1. Move of all services to a common IP network means '*Attack surface Area*' is correspondingly increased
2. Separate ring-fenced SS No 7 signalling network swapped for common SIP system
3. Move to virtualisation of network functions
4. Move of functions to cloud
5. Introduction of Open network APIs
6. Subs using new IP IoT (vulnerable via WiFi, etc] for alarms

5G Network Architecture (Functional)



3. Issues with all-IP networks

Move Towards Consolidated IP Core

1. Consolidating onto unified Core Networks to absorb stand-alone 5G and Intelligent Fixed core (i.e. NGN)
 - a) 5G stand-alone Core
 - b) Closure of PSTN and shift of voice to fixed NGN
 - c) Closure of many legacy transport (transmission and data packet platforms)
 - d) Shift of functions to cloud support
 - e) Introduction of network slicing
 - f) Introduction of SDN and NFV

2. This leads to simplification in network operations
 - Fewer technologies to support
 - Easier dimensioning of networks

Cost Savings:

 - *Lower opex*
 - *Lower capex*

3. Potential new services

} *New revenues*

Telecoms Operator's IP Networks are Under Constant Attack!

News item in the UK's Guardian newspaper
two weeks ago (13th September 2024) 

anges
vere
e" or
ent".
ased
and
aid.
ow-
t for
zed

MEs
ing
ion
the
ss,"

esi-
the

the
nt
ro-
he

ed
m-
to
to
g
1-

BT identifying 2,000 signals a second that could indicate cyber-attacks

Mark Sweney

BT identifies 2,000 signals indicating a potential cyber-attack across its networks every second, it has revealed, amid an "AI arms race" between businesses bolstering their defences and increasingly sophisticated hackers.

The telecoms company - owner of the mobile operator EE and Openreach, which has the biggest broadband network in the UK - said hackers were attempting to weaponise AI for cybercrime.

In the past year, BT's digital surveillance of its networks has identified an increase of more than 1,200% in new malicious signals.

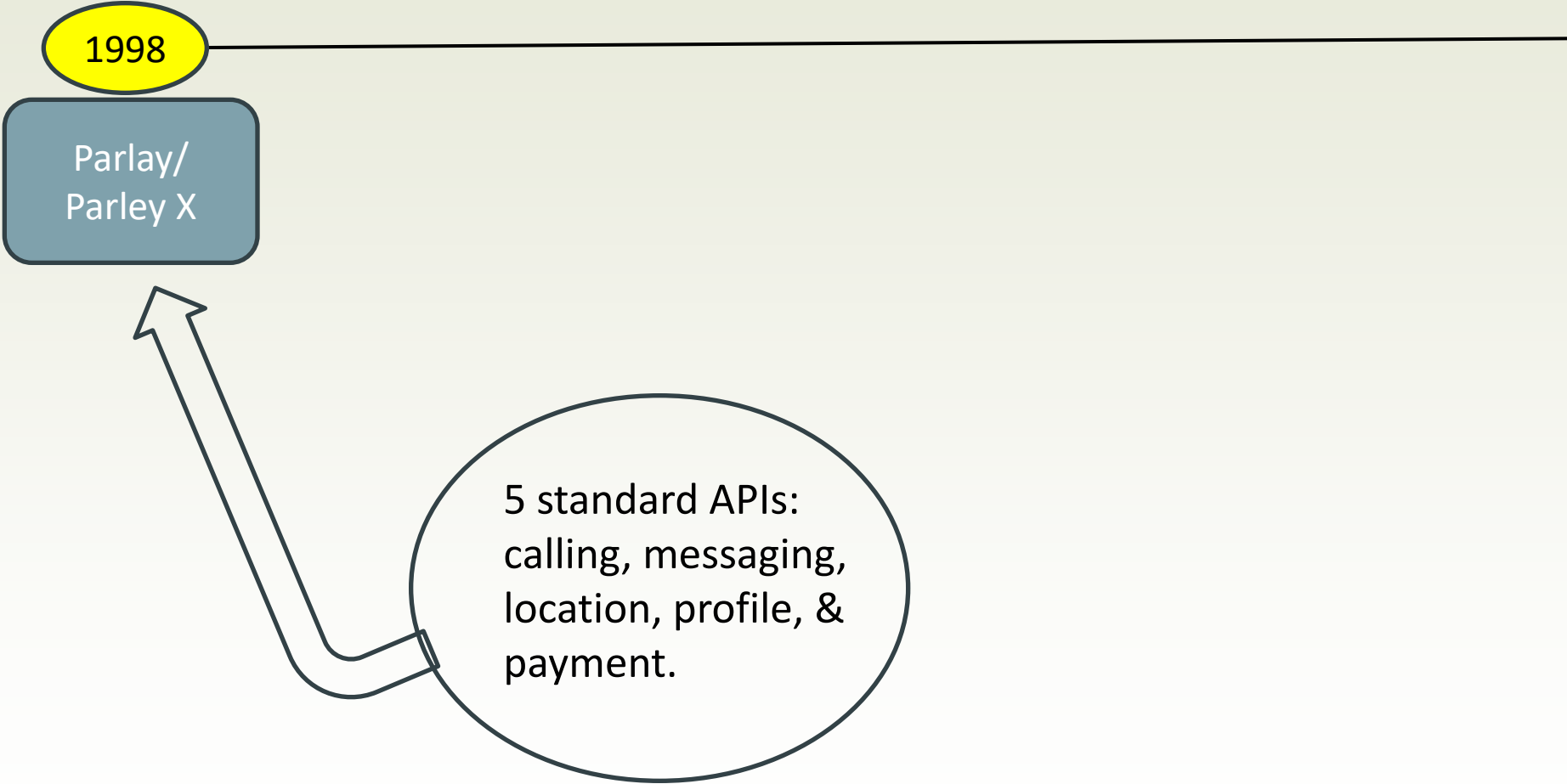
4. Opening of Operators' Networks

The Opening Up of the Telecom Network

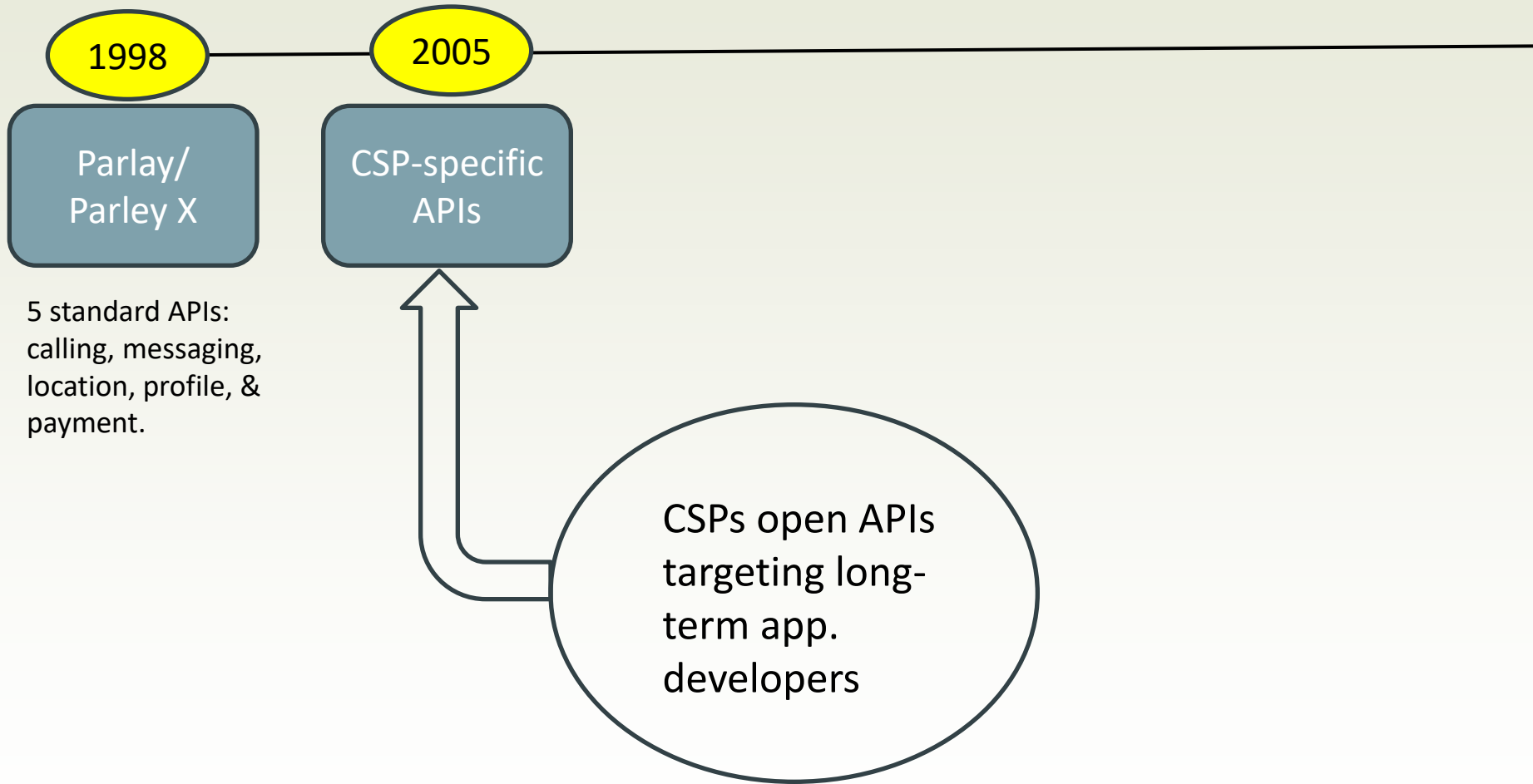
1998

Parlay/
Parlay X

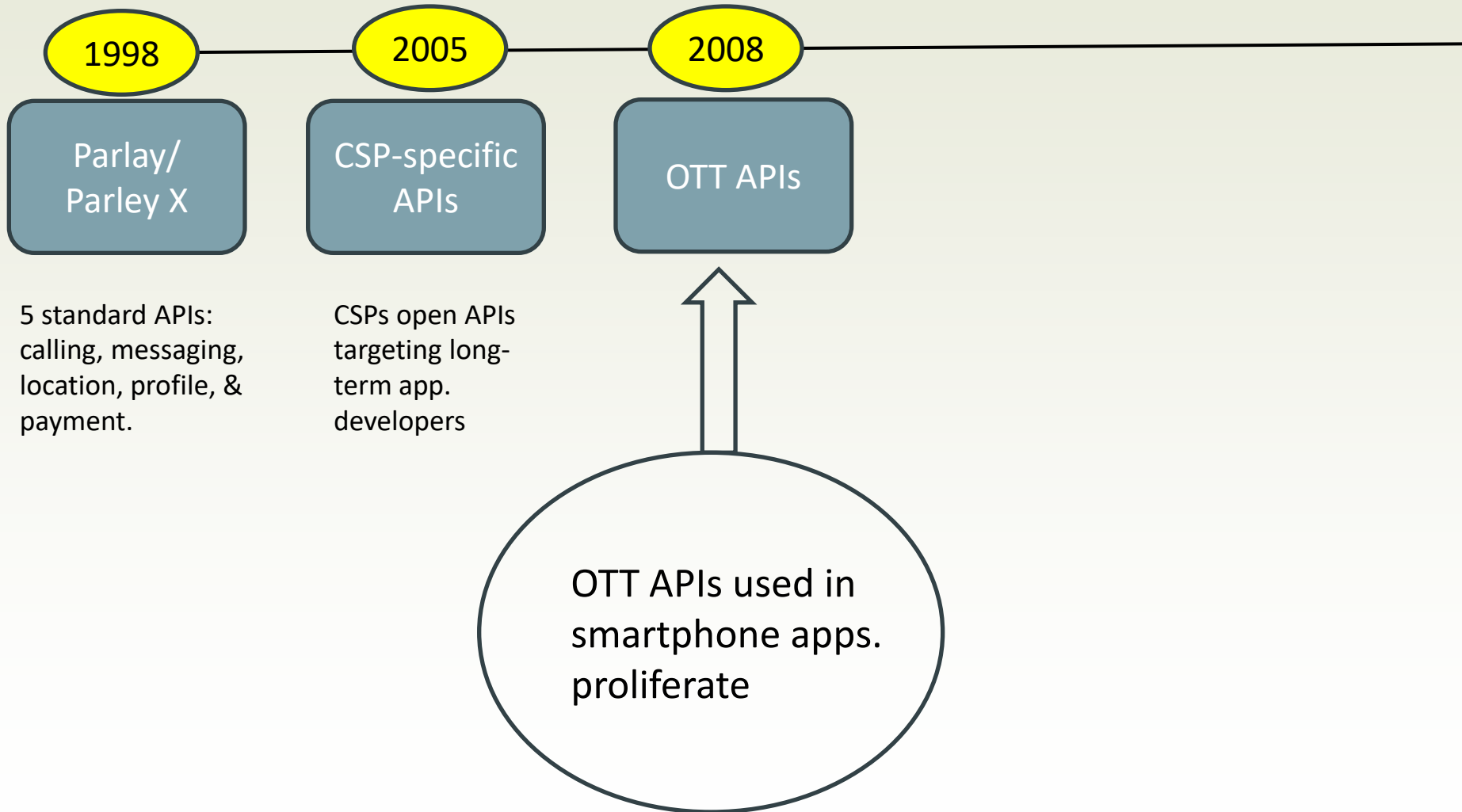
5 standard APIs:
calling, messaging,
location, profile, &
payment.



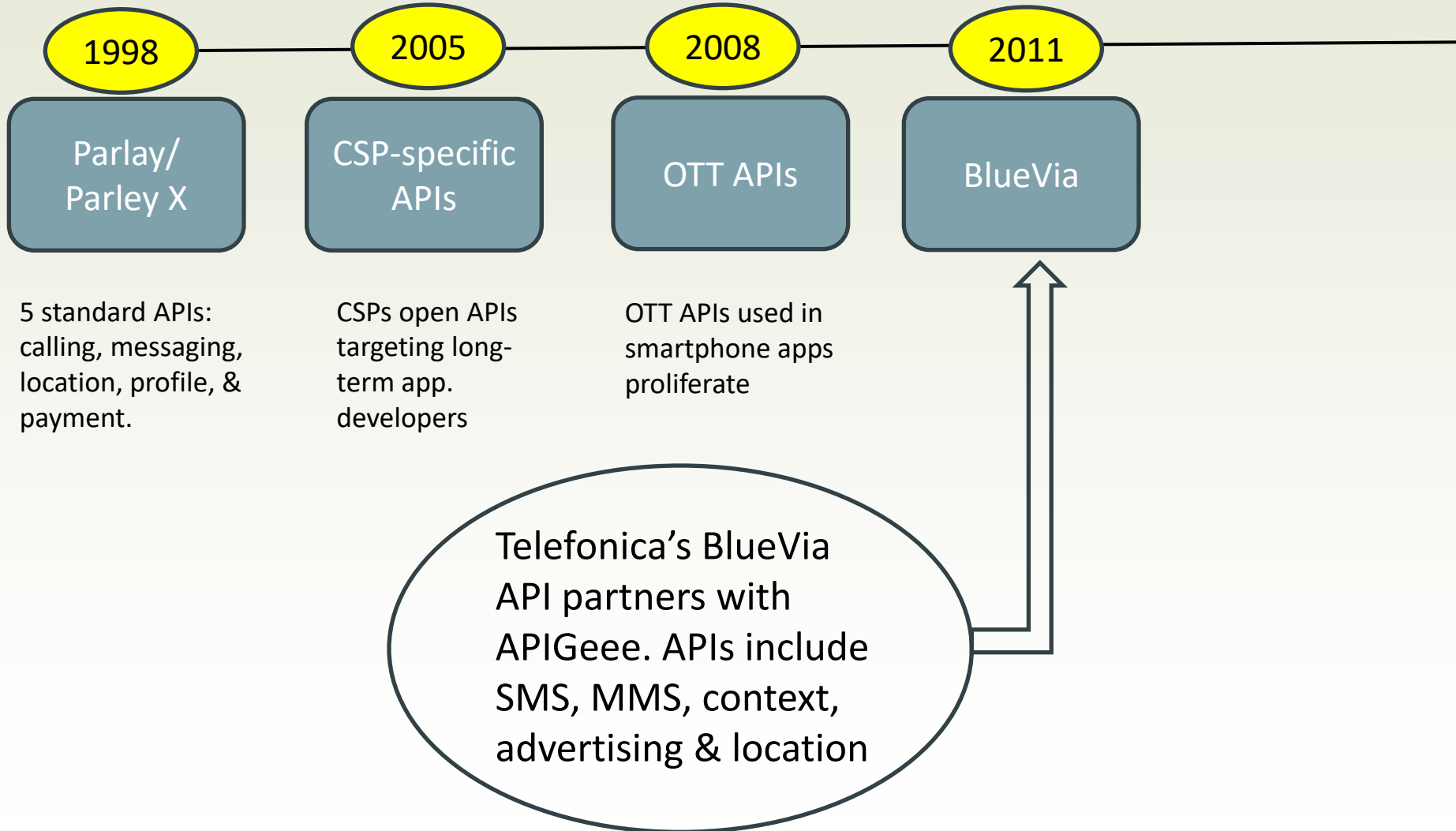
The Opening Up of the Telecom Network



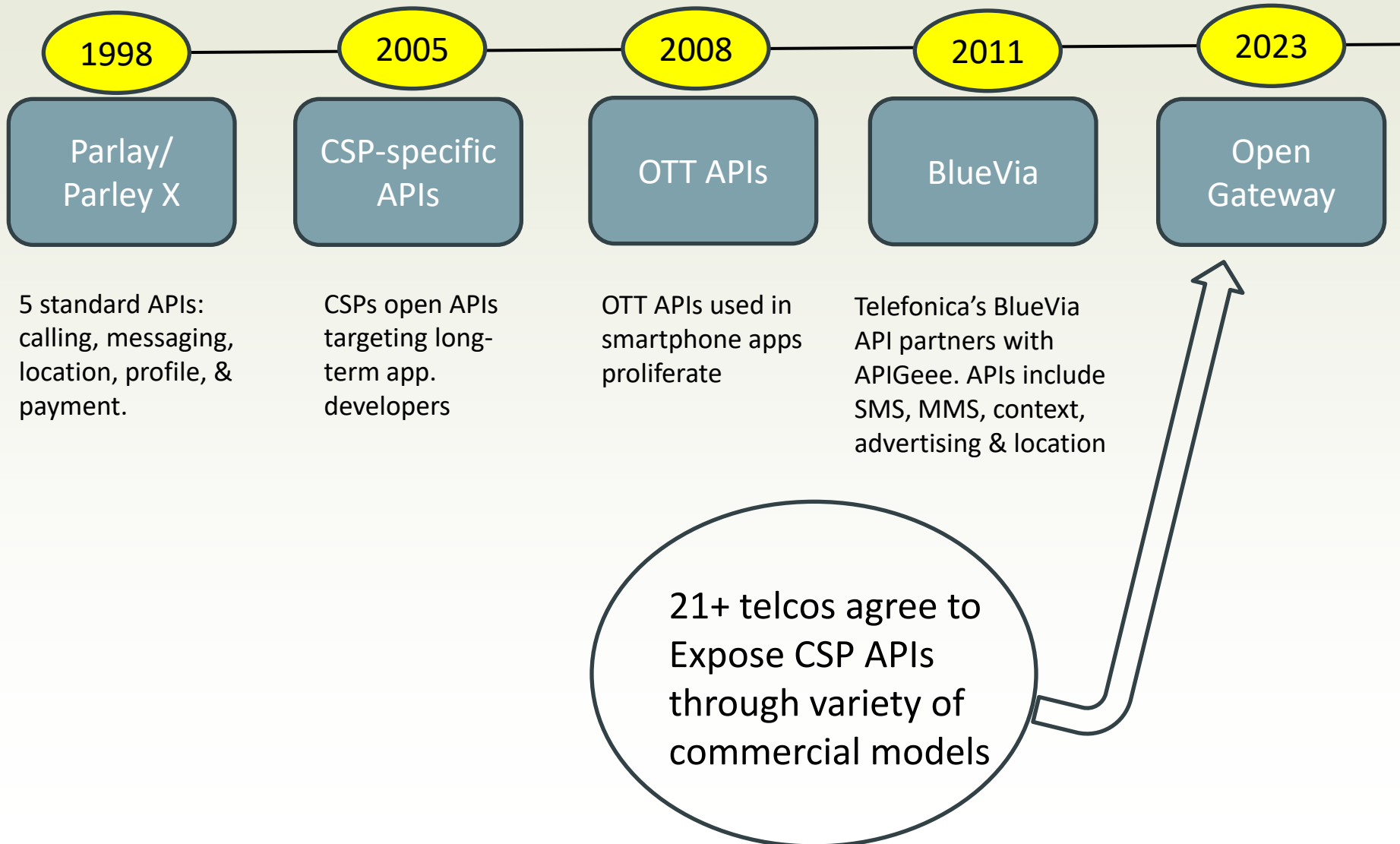
The Opening Up of the Telecom Network



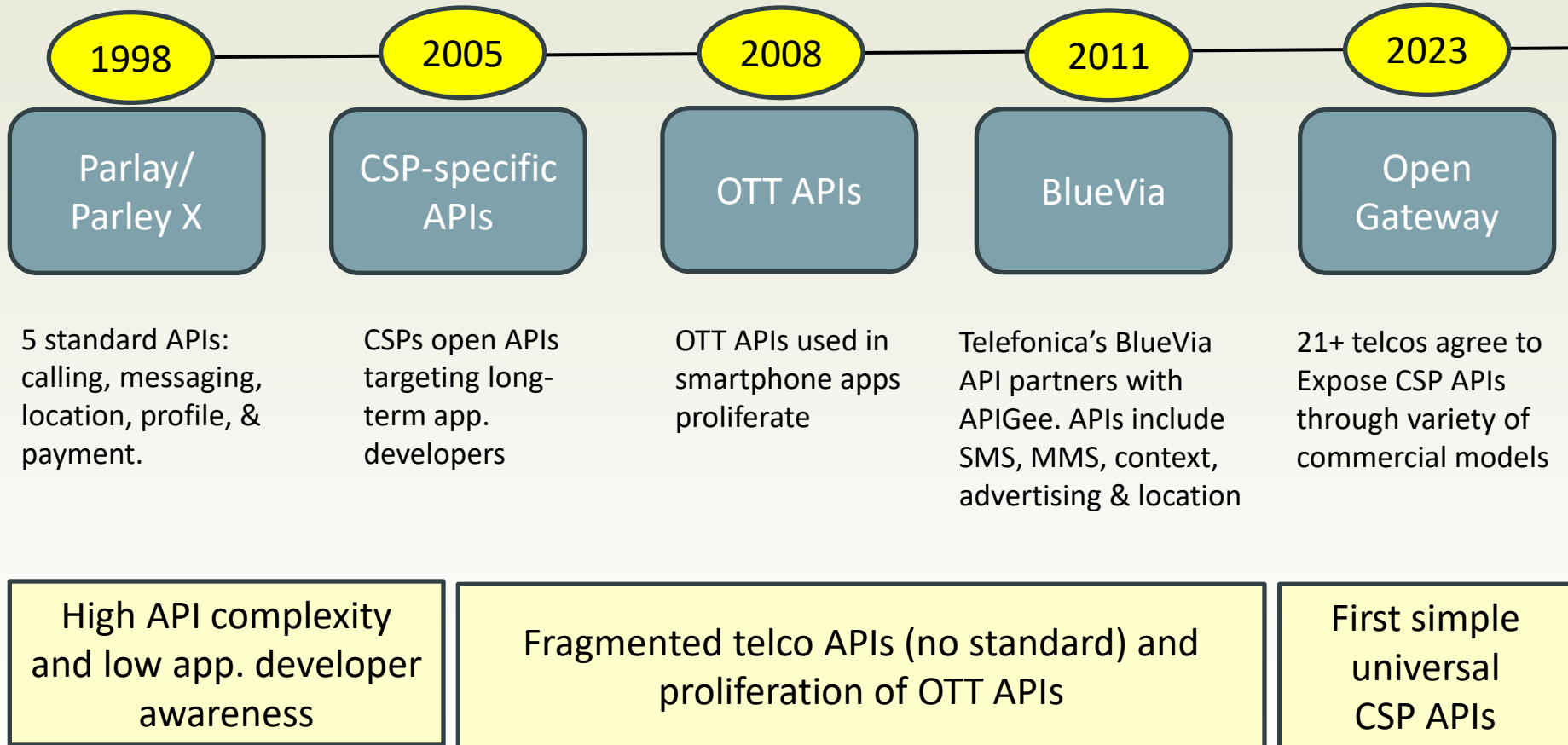
The Opening Up of the Telecom Network



The Opening Up of the Telecom Network



The Opening Up of the Telecom Network



GSMA 'Open Gateway' Initiative

Launched at MWC 2023 with the support of 21 Global MNOs:

- Defined as 'a framework of universal APIs designed to provide universal access to operators' networks for application developers'
- One of the main themes at MWC 2024
- *"....by federating open network APIs and applying interoperable roaming concept, mobile operators and cloud services will be truly integrated to enable new world of opportunity". CEO Telefonica.*

CAMARA is an open-source LINUX project to define, develop, test and publish APIs in collaboration with GSMA.

Types of Network APIs

Network Information APIs

- Location verification
- Identity API family
 - Know your customer
 - Number verification

Some 21 use cases
now Identified

Network Configuration APIs

- Configuration instructions
 - QoS (bandwidth, latency)
 - Network slicing (by time, on demand)

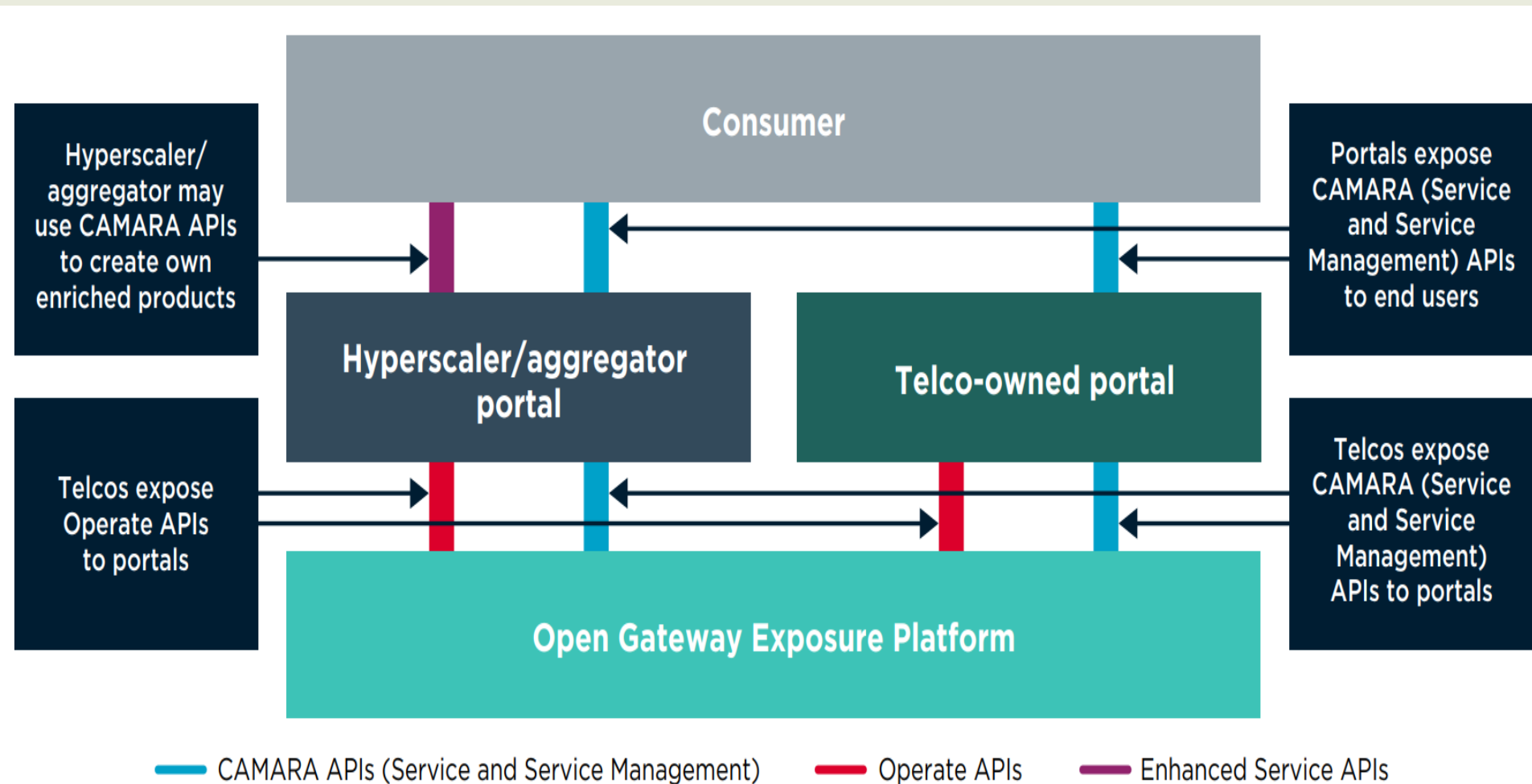
Other Network APIs

- Direct carrier billing
- Adaptive cloud usage

Progress of development

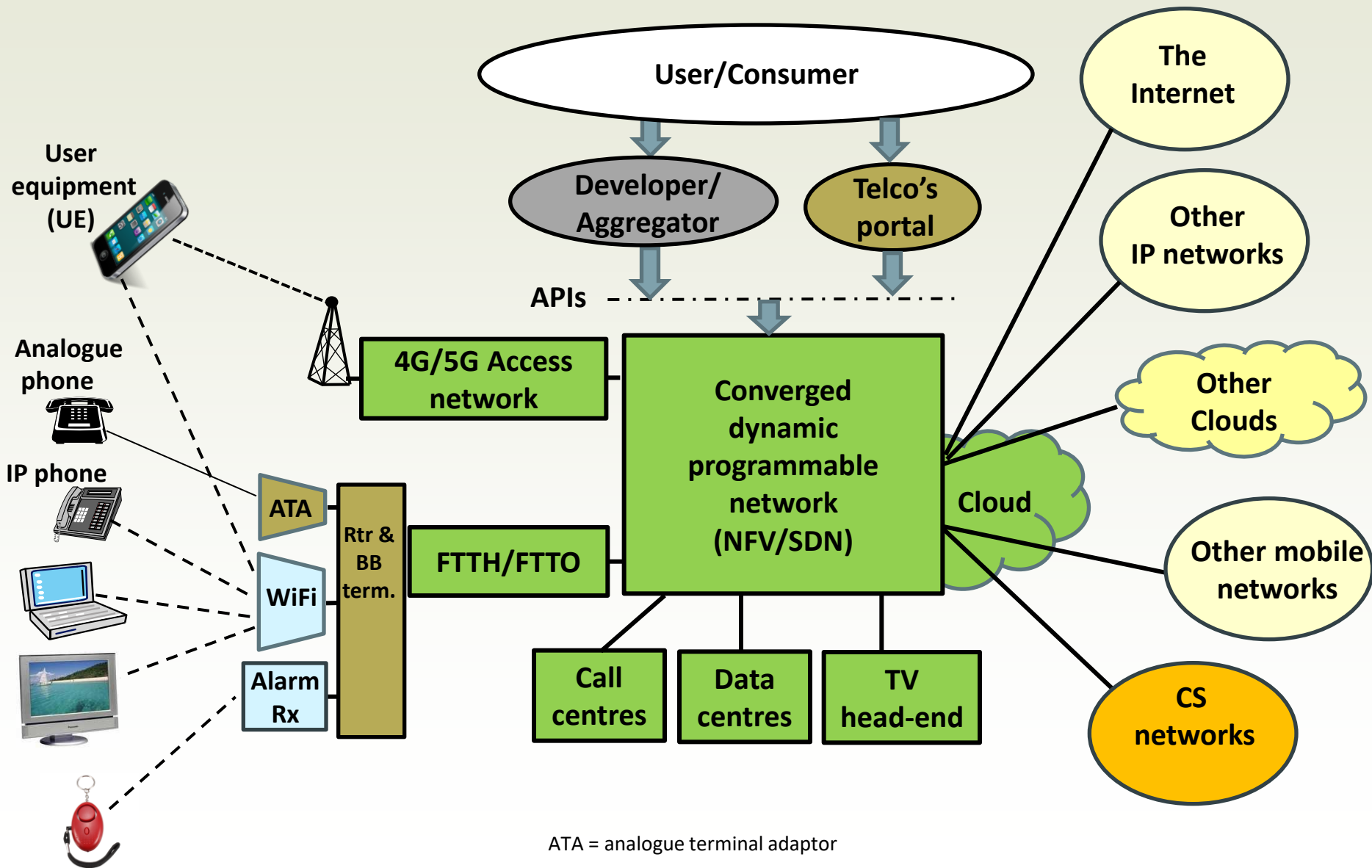


API Stakeholder Architecture & Relationships



4. Conclusions

The Emerging All-IP Network Ecosystem



ATA = analogue terminal adaptor

In Conclusion

Closing the PSTN and transferring all the (fixed) voice and non-voice services on to an all-IP common services network:

- (a) increases the spread of different services sharing the common network;*
- (b) introduces additional security vulnerabilities to the “non-digital” users.*

Thank you

a.valdar@ucl.ac.uk