ISSE 2014
14th & 15th October 2014
MCE, Brussels, Belgium
www.isse.eu.com
Securing Assets Across Europe

Schengen routing or Schengen encryption?

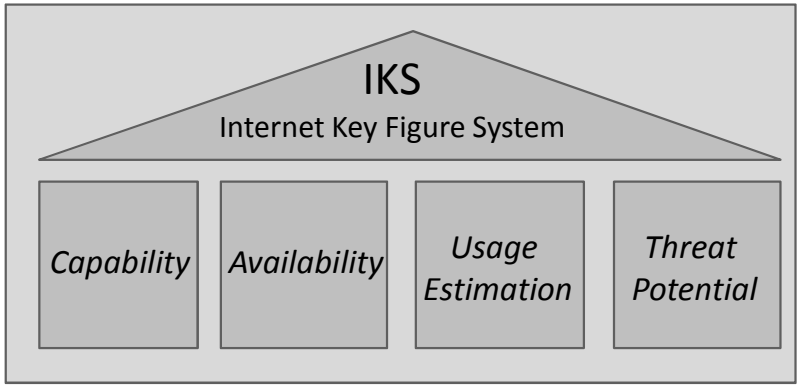
Secure communication and digital sovereignty in Europe

Prof. Norbert Pohlmann

if(is) internet security.

Internet Key Figure System (IKS)
→ act with the right key figure

- IKS performs
  continuous measurements
  of the main technical parameters
  of the Internet
  in various functional segments.



- Technical indicators are calculated from the variety of raw data in order to
  - enhance transparency of complex relationships
  - show long-term developments.

- More than 100 million characteristics are generated in the area of Internet infrastructure (capability) annually

The Internet Infrastructure
→ actual key indicators

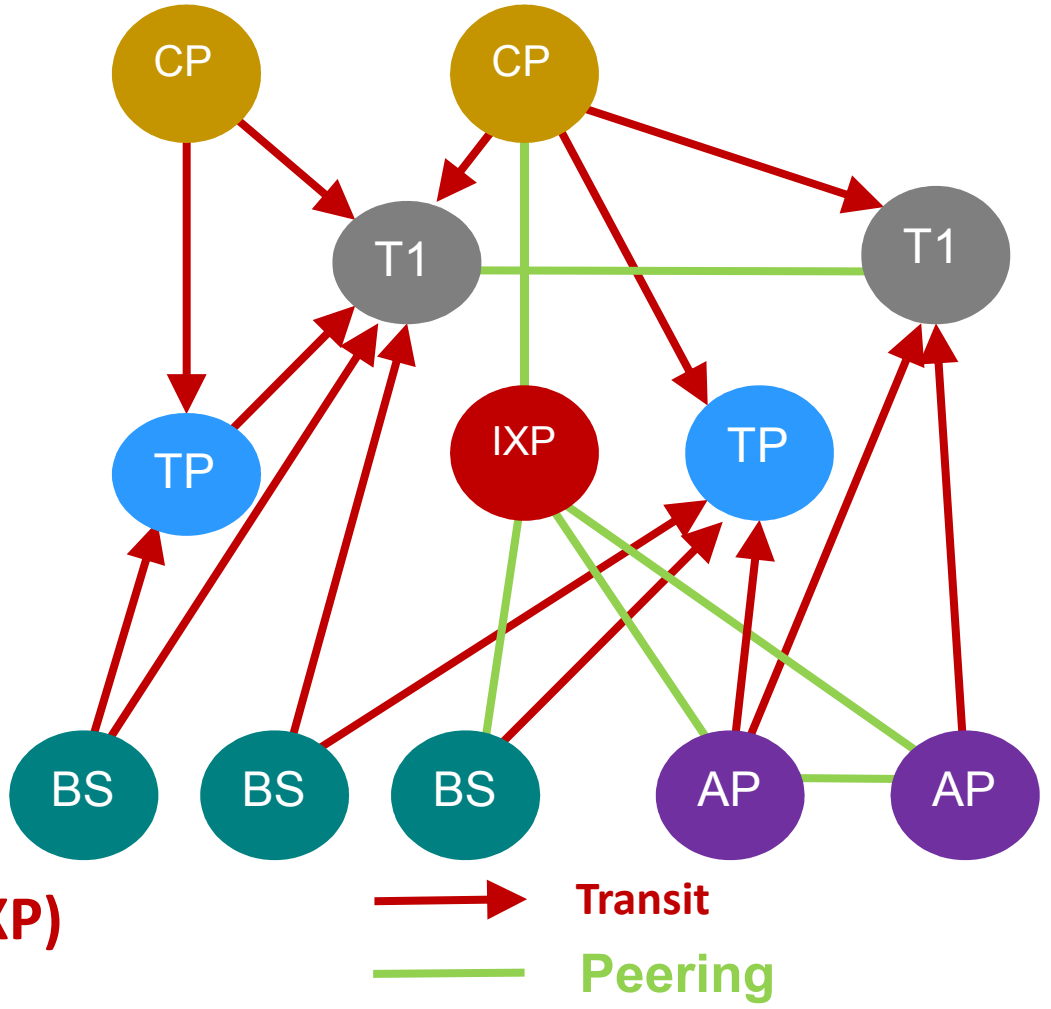
The **Internet** is a non-homogeneous, decentralized and geographically asymmetrical distributed network of **managed sub-nets**, called "**autonomous systems**" (AS)

Key indicators of current Internet infrastructure:

- 50,000 autonomous systems worldwide, e.g. 1,500 in Germany; 15,000 in the USA
- 234 countries
- 500,000 logical connections between AS
- 50% of all connections are attributed to G20 member states

Structure of the Internet
→ if(is) model: Types of AS

- Tier 1 Network (T1)
- Transit Provider (TP)
- Content Provider (CP)
- Access Provider (AP)
- Business Customers AS (BS)
- Internet Exchange Points (IXP)



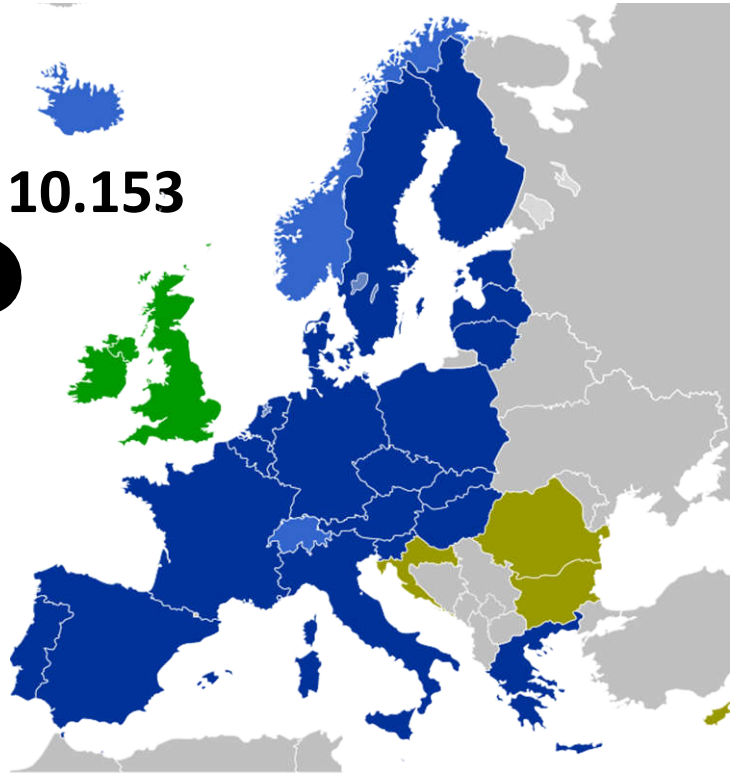
Schengen / Schengen Net
→ facts and figures

- The Schengen area includes 26 countries:

  Austria, Belgium, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and Switzerland.

- The number of AS in **"Schengen Net"**: **10.153**
  (20 % of the global amount) (1/2014)

- The number of connections in "Schengen Net": **136.783**
  (27 % of the global amount)



Categorization of autonomous systems

	ISO	Country	Access	Transit	Content	Business	∑
1	AT	Austria	44	88	40	344	465
2	BE	Belgium	11	41	35	143	195
3	CH	Switzerland	33	110	50	438	578
4	CZ	CzechRepublic	22	108	55	294	424
5	DE	Germany	**126**	**315**	**253**	1048	1494
6	DK	Denmark	25	34	37	180	229
7	EE	Estonia	6	17	12	36	59
8	ES	Spain	30	52	88	402	489
9	FI	Finland	28	22	35	156	193
10	FR	France	76	176	142	651	915
11	GR	Greece	20	12	15	129	150
12	HU	Hungary	19	34	34	139	203
13	IS	Iceland	3	20	12	24	47
14	IT	Italy	45	127	95	510	703
15	LI	Liechtenstein	0	6	0	9	17
16	LT	Lithuania	9	25	17	77	109
17	LU	Luxembourg	4	20	7	26	52
18	LV	Latvia	5	30	23	171	224
19	MT	Malta	2	6	3	19	28
20	NL	Netherlands	67	233	147	356	659
21	NO	Norway	30	62	30	119	195
22	PL	Poland	41	148	88	**1347**	**1754**
23	PT	Portugal	15	17	15	52	72
24	SE	Sweden	47	103	58	365	517
25	SI	Slovenia	11	21	17	236	260
26	SK	Slovakia	7	43	13	77	128

"Schengen Net"

all 26 „Country Internets" of the Schengen countries belong to Schengen Net

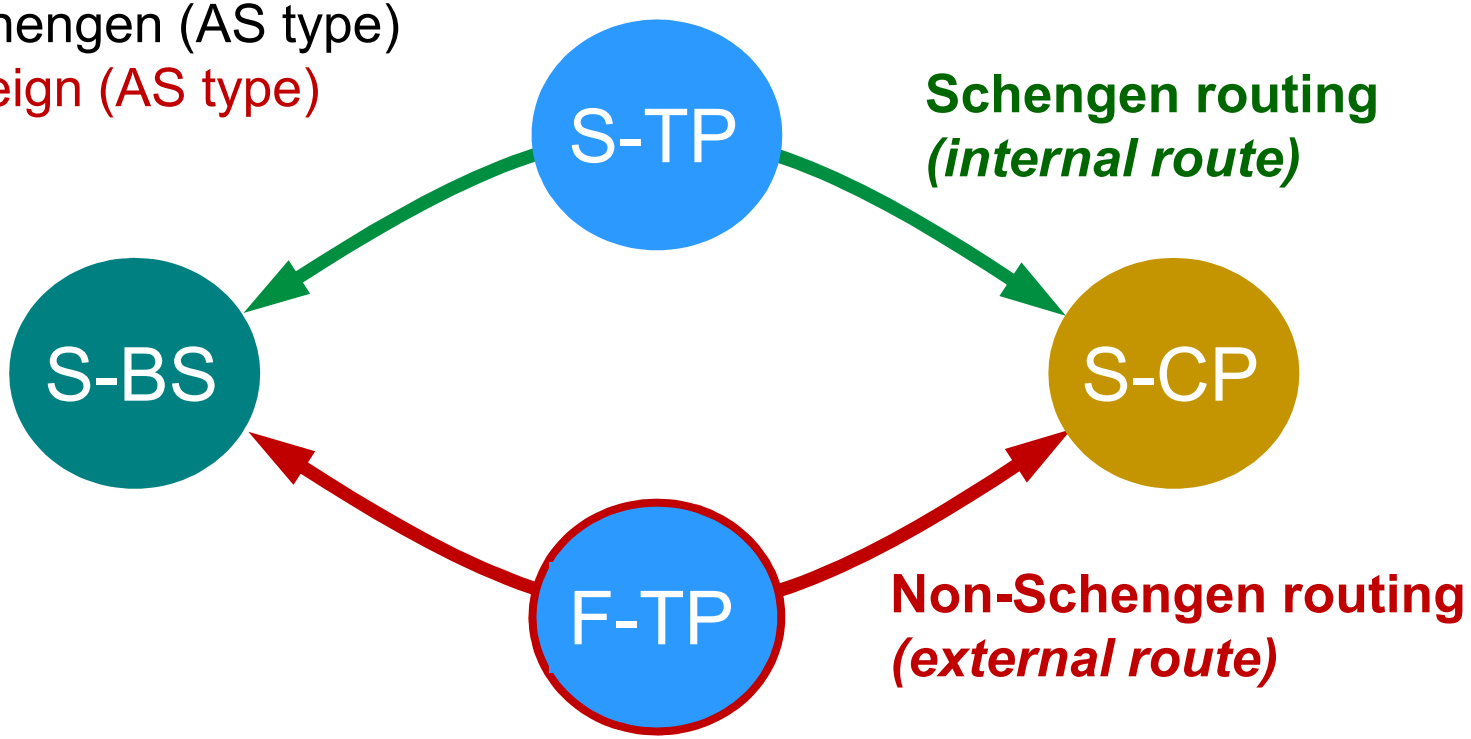
„Country Internet"

AT, BE, CH, CZ, DE, …

The core set of a ***country's AS*** is comprised of networks (AS) that have ***the majority of IP addresses*** located there.

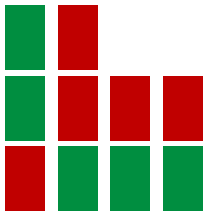
Schengen Routing
→ basic Idea

S: Schengen (AS type)
F: foreign (AS type)

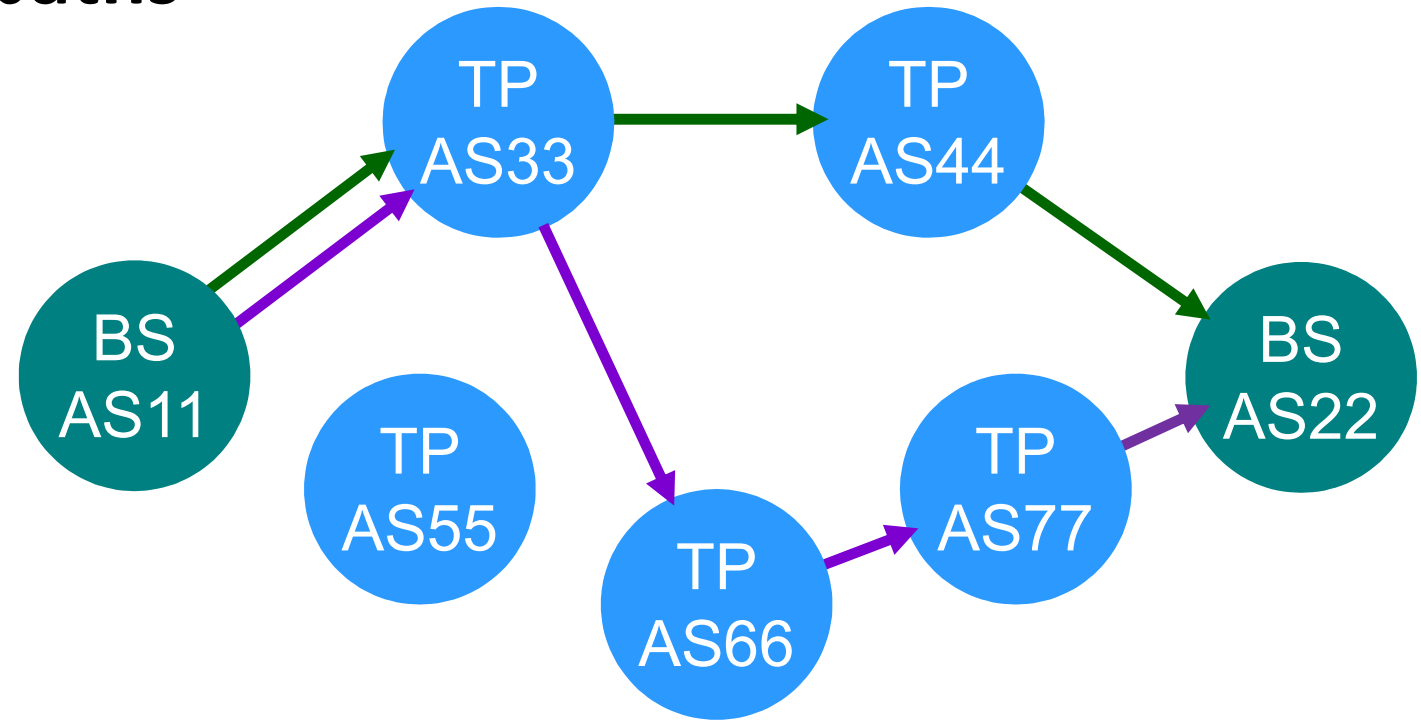


Criteria for the routing choice

→ Quality of Service
→ Pricing model
→ Trustworthiness



Border Gateway Protocol (BGP)
→ paths



The IP packet must pass through an **AS-Path** to reach its destination *(e.g. from **AS11** to **AS22**)*

→ **AS 33 66 77 22** *(one possible paths)*

→ **AS 33 44 22** ***(shortest paths)***

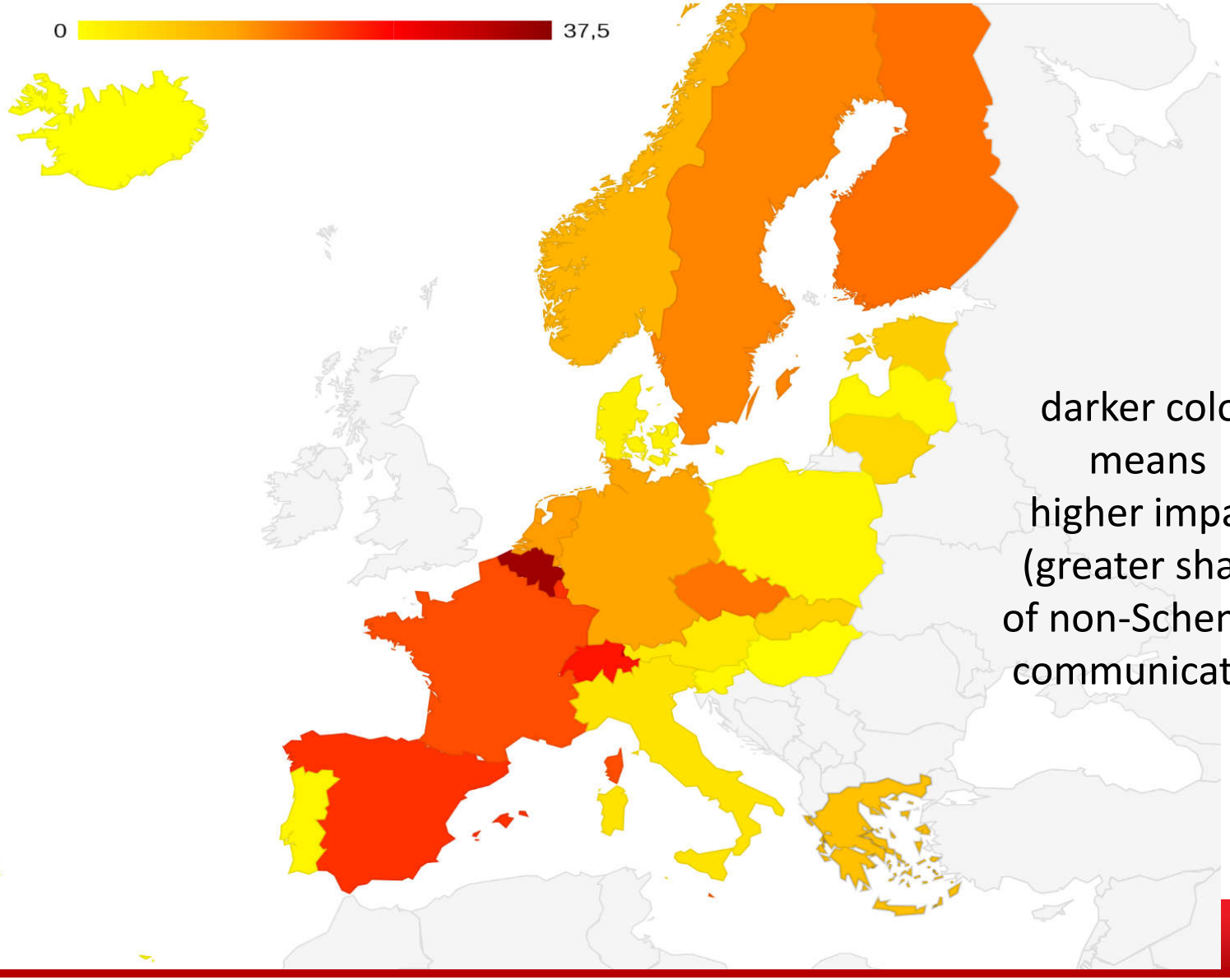
Simulation of a restricted routing model → analysis of paths

- **Question:** Which paths are most frequently utilized for the transport of IP packets from start to destination AS?
- **Assumption:** The shortest paths are preferred (Shortest Path Strategy)
- **Analysis methodology:**
  - Analysis of **all publicly visible** paths between all Schengen AS
  - Statistical separation of Schengen and non-Schengen routes

Schengen routes: All AS in the respective path are located within Schengen area, including source and destination AS

non-Schengen routes: One or more AS in the respective path are located outside the Schengen area, whereas both source and destination AS are located within Schengen area.

Key results of analysis
→ Schengen routing



darker color means higher impact (greater share of non-Schengen communication)

Estimated impact

	ISO	Country	Score Schengen	Score Country	AS Country
1	BE	Belgium	35,38	49,32	195
2	LI	Liechtenstein	29,41	42,91	17
3	CH	Switzerland	23,48	35,45	578
4	ES	Spain	21,27	31,77	489
5	LU	Luxembourg	21,15	35,87	52
6	FR	France	19,13	30,22	915
7	MT	Malta	17,86	31,89	28
8	FI	Finland	16,58	23,45	193
9	CZ	CzechRepublic	16,31	30,70	424
10	SE	Sweden	14,92	25,24	517
11	NL	Netherlands	13,07	23,48	659
12	DE	Germany	12,26	22,21	1494
13	NO	Norway	10,31	18,42	195
14	GR	Greece	8,67	15,17	150
15	EE	Estonia	6,78	14,54	59
16	SK	Slovakia	6,25	12,19	128
17	LT	Lithuania	5,50	10,64	109
18	IT	Italy	3,70	8,15	703
19	AT	Austria	3,23	7,54	465
20	DK	Denmark	1,75	4,21	229
21	PL	Poland	1,43	3,80	1754
22	PT	Portugal	1,39	4,55	72
23	LV	Latvia	1,34	3,24	224
24	SI	Slovenia	1,15	2,34	260
25	HU	Hungary	0,49	2,22	203
26	IS	Iceland	0,00	0,00	47

Very high impact
(20+ % of data communication is routed via non-Schengen AS
35+ % via foreign country)

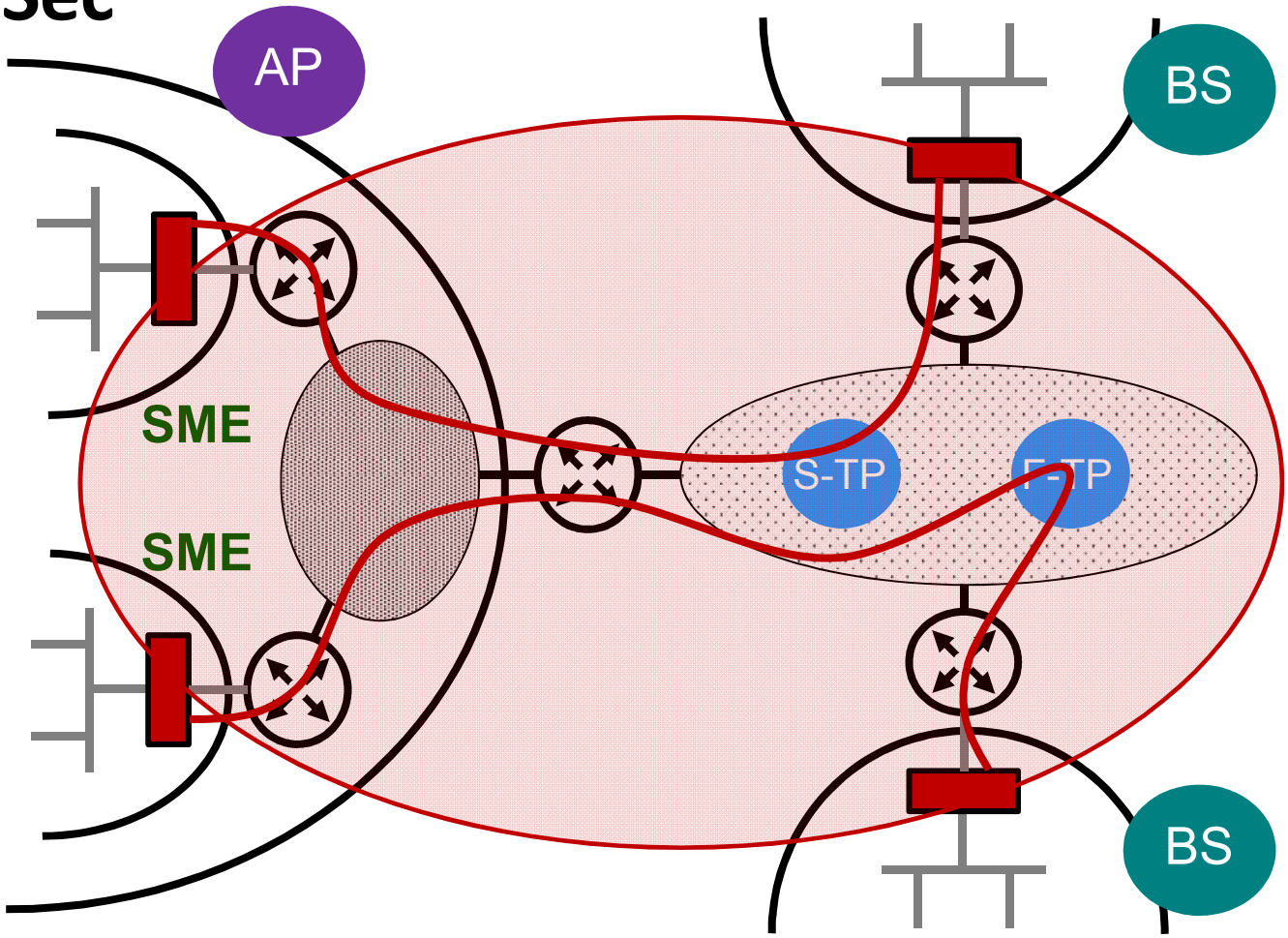
Evaluation of the concept → of routing restrictions

- We see “no change” to “high impact” **affects in the different Schengen countries**.
- **Restrictions** on the Schengen traffic **impede the provider competition** and **degrade the robustness**.
- **Investment** in infrastructure Schengen **becomes less attractive** (for non-Schengen Provider → market leaders).
- Reduced competition may lead to **price increases**.
- Pitfalls of regional AS categorization are affecting the results of analysis (Global companies: Siemens, Shell, ...)
- **Foreign communication is necessary in the global Internet!**
- **Connections between autonomous systems** are prone to technical interception regardless of regional policies or preferences.

Active Encryption
→ Much more is needed

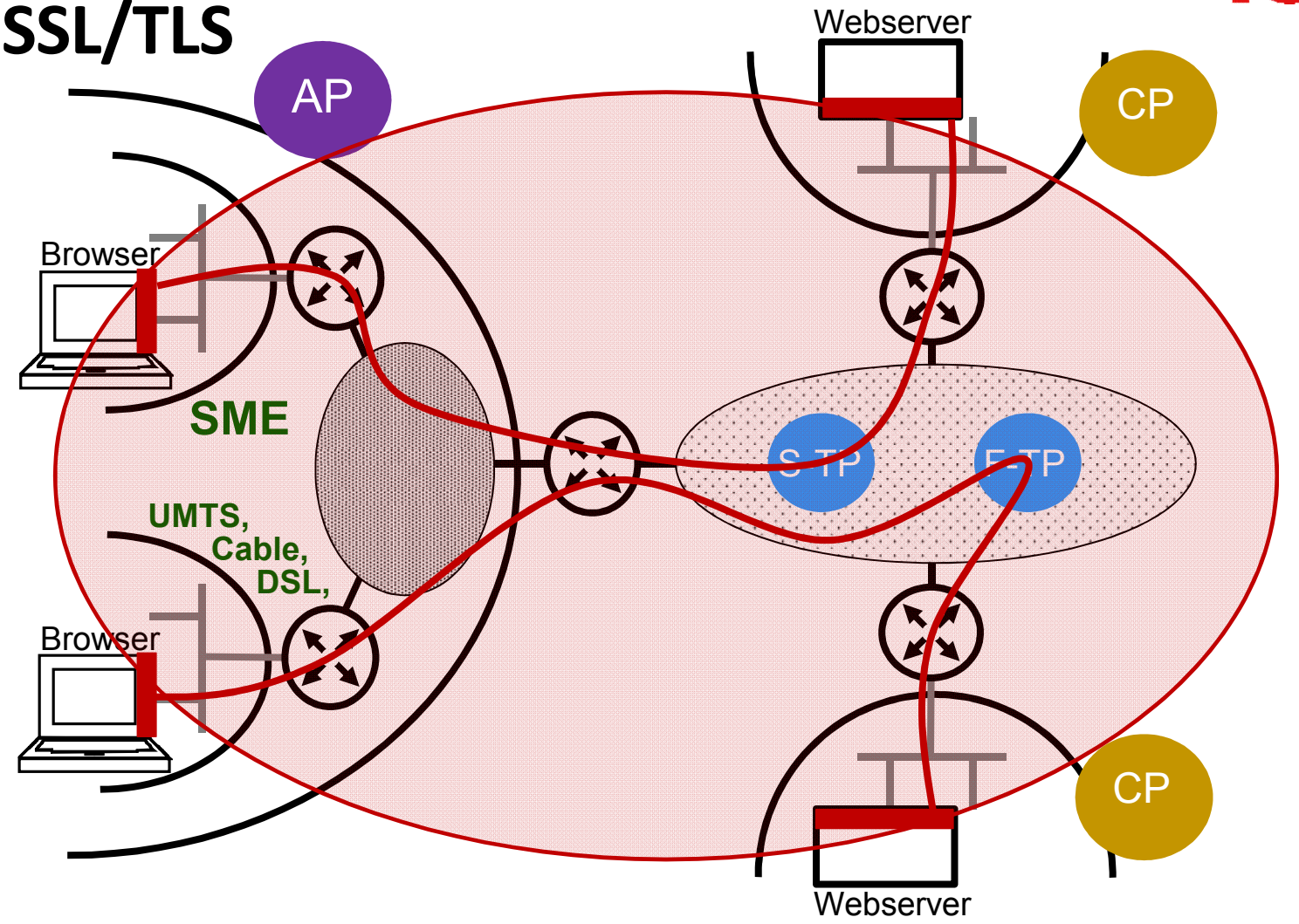
- Encryption for a **sustainable protection of our data** (data centers of the Autonomous Systems + cable, wireless, ...)
- A discussion of an own router technology in Europe (digital sovereignty) would no longer be necessary if we encrypt all data!
- **Requirements:**
  - **Trustworthy encryption technology** (No backdoors, strong random numbers, correct implementation, ...)
    → Very powerful IT security industry in Schengen area
    → IT Security made in Europe
  - **Trustworthy IT security infrastructures** (PKI with RA und CA; Root certificates, …)

Encryption
→ IPSec



Every 125th IP packed in the Internet is IPSec encrypted at the moment
(trend is rising)

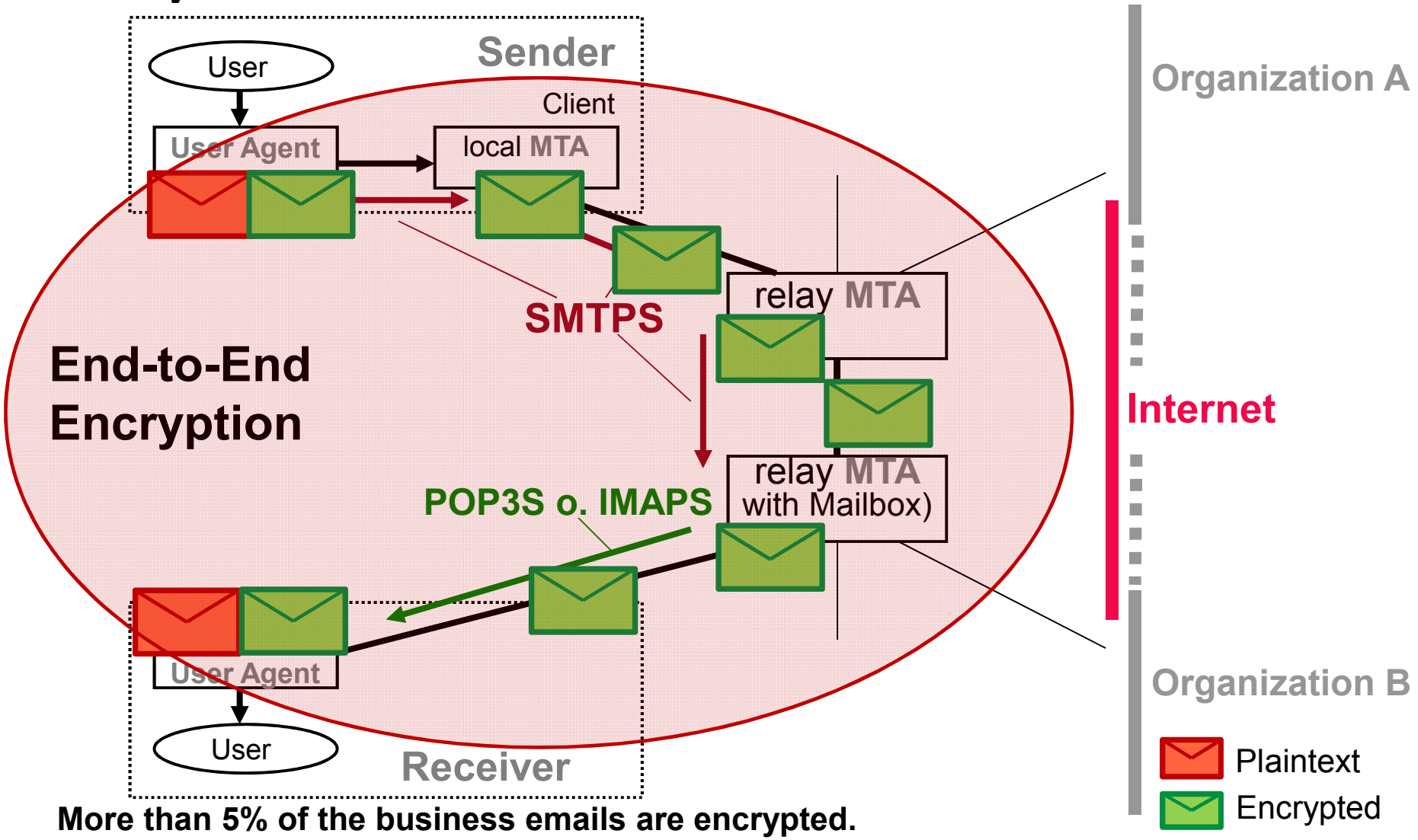
Encryption
→ SSL/TLS



Every 7th IP packed in the Internet is SSL/TLS encrypted

(SSL/TLS (Port 443) 23 % and HTTP (Port 80) 77 % - trend is rising)

Encryption
→ S/MINME or PGP



More than 5% of the business emails are encrypted.
(trend is rising, but not in the sky)

Schengen Routing or Encryption?
→ Conclusion

- We discussed two basic concepts for **secure communication** and **digital sovereignty** in Europe.
- **Concept of local routing restrictions**
  (limiting data traffic to Schengen area of common data protection regulation)
- **Concept of applying cryptography to data traffic**
  (encryption of data in the Schengen area and above)
- Routing restrictions are suffering from conceptual shortcomings (policy-related approach, no proven security enhancements)
- **Complete encryption** of the data traffic seems to be **the most sensible approach**!

ISSE 2014
14th & 15th October 2014
MCE, Brussels, Belgium
www.isse.eu.com
Securing Assets Across Europe

Schengen routing or Schengen encryption?

Secure communication and digital sovereignty in Europe

Let us encrypt the data in Europe!

Prof. Norbert Pohlmann

if(is) internet security.