

SDN-based Network Obfuscation

Master Thesis
Roland Meier

Tutor: Dr. David Gugelmann

Supervisor: Prof. Dr. Laurent Vanbever

The image shows two news articles side-by-side. The left article is from the *Neue Zürcher Zeitung* (NZZ) with the title "Britischer Lauschangriff im Internet" and "Interkontinentale Glasfaserkabel in riesigem Ausmass angezapft". It includes a snippet of text: "In Grossbritannien wird laut einem Zeitungsbericht U Hinweisen Snowdens der interkontinentale Internet Telefonverkehr systematisch abgehört. Das könnte". The right article is from *The Atlantic* with the title "The Creepy, Long-Standing Practice of Undersea Cable Tapping". It includes a snippet of text: "The newest NSA leaks reveal that governments are probing 'the Internet's backbone.' How does that work?" Both articles are dated 23.6.2013, 21:23 Uhr.

Neue Zürcher Zeitung

Britischer Lauschangriff im Internet

Interkontinentale Glasfaserkabel in riesigem Ausmass angezapft

von Peter Rásonyi, London / 23.6.2013, 21:23 Uhr

In Grossbritannien wird laut einem Zeitungsbericht U Hinweisen Snowdens der interkontinentale Internet Telefonverkehr systematisch abgehört. Das könnte

The Atlantic

SUBSCRIBE SEARCH MENU

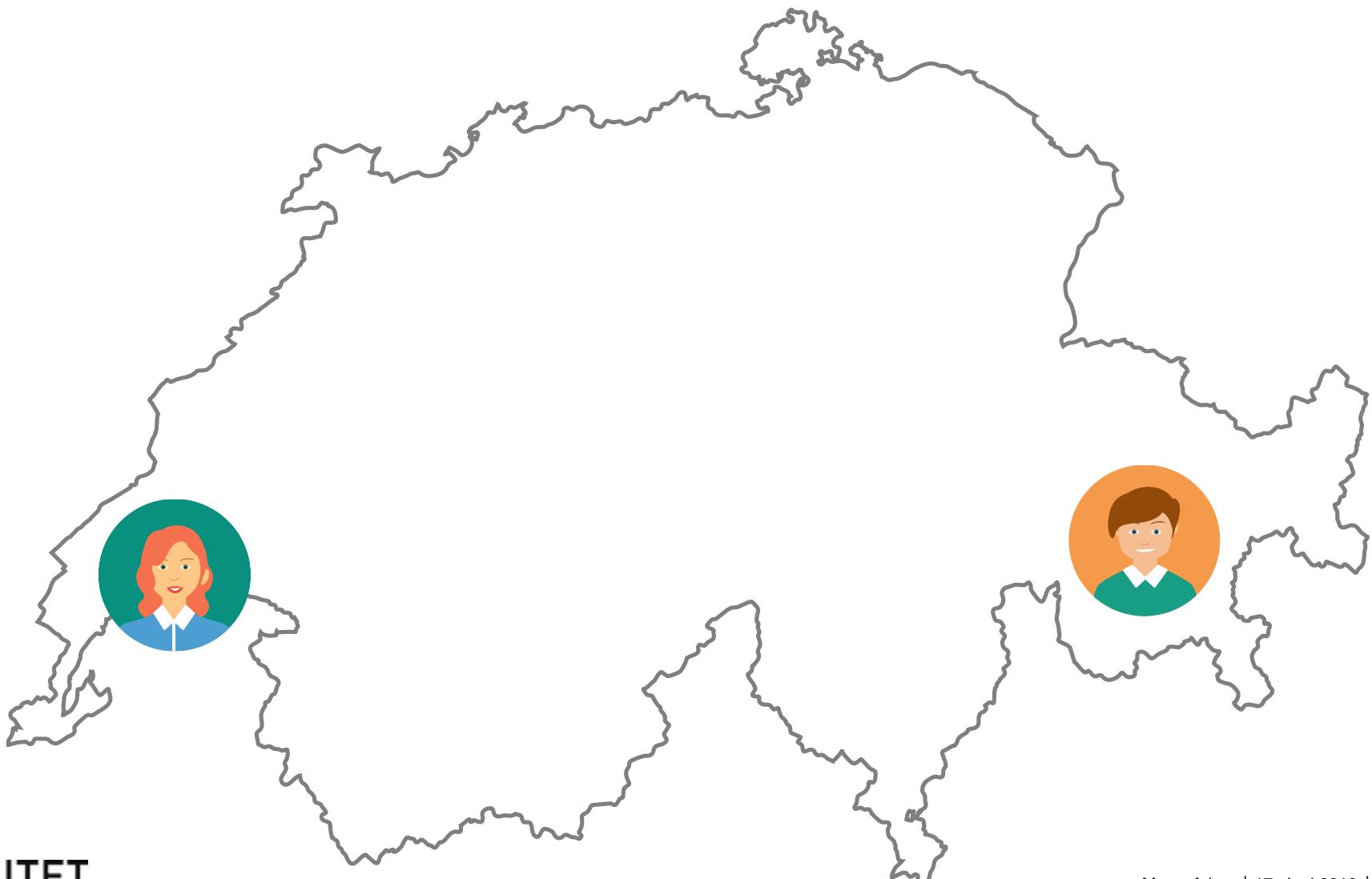
GLOBAL

The Creepy, Long-Standing Practice of Undersea Cable Tapping

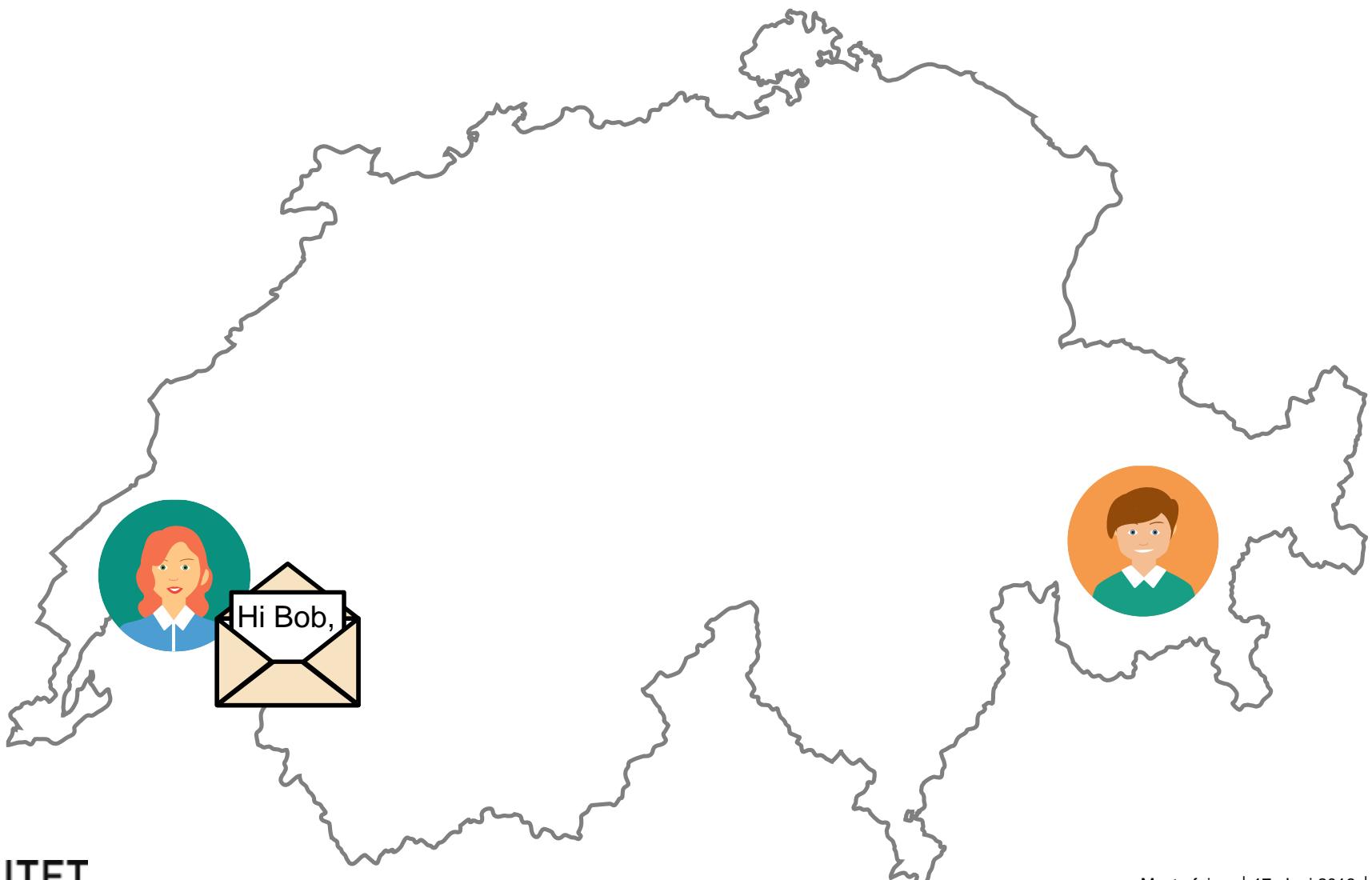
The newest NSA leaks reveal that governments are probing "the Internet's backbone." How does that work?

OLGA KHAZAN | JUL 16, 2013

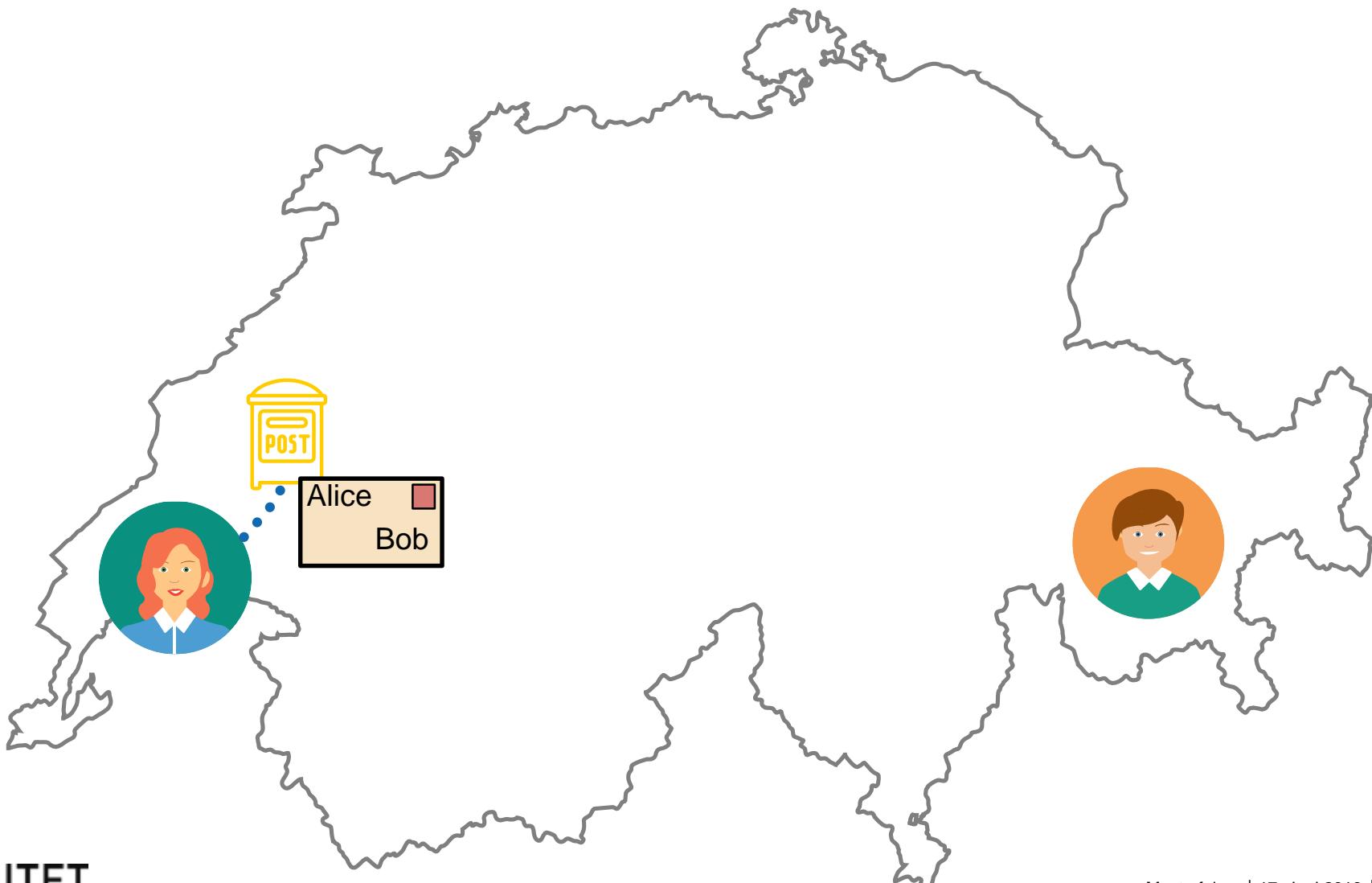
A story about Alice and Bob...



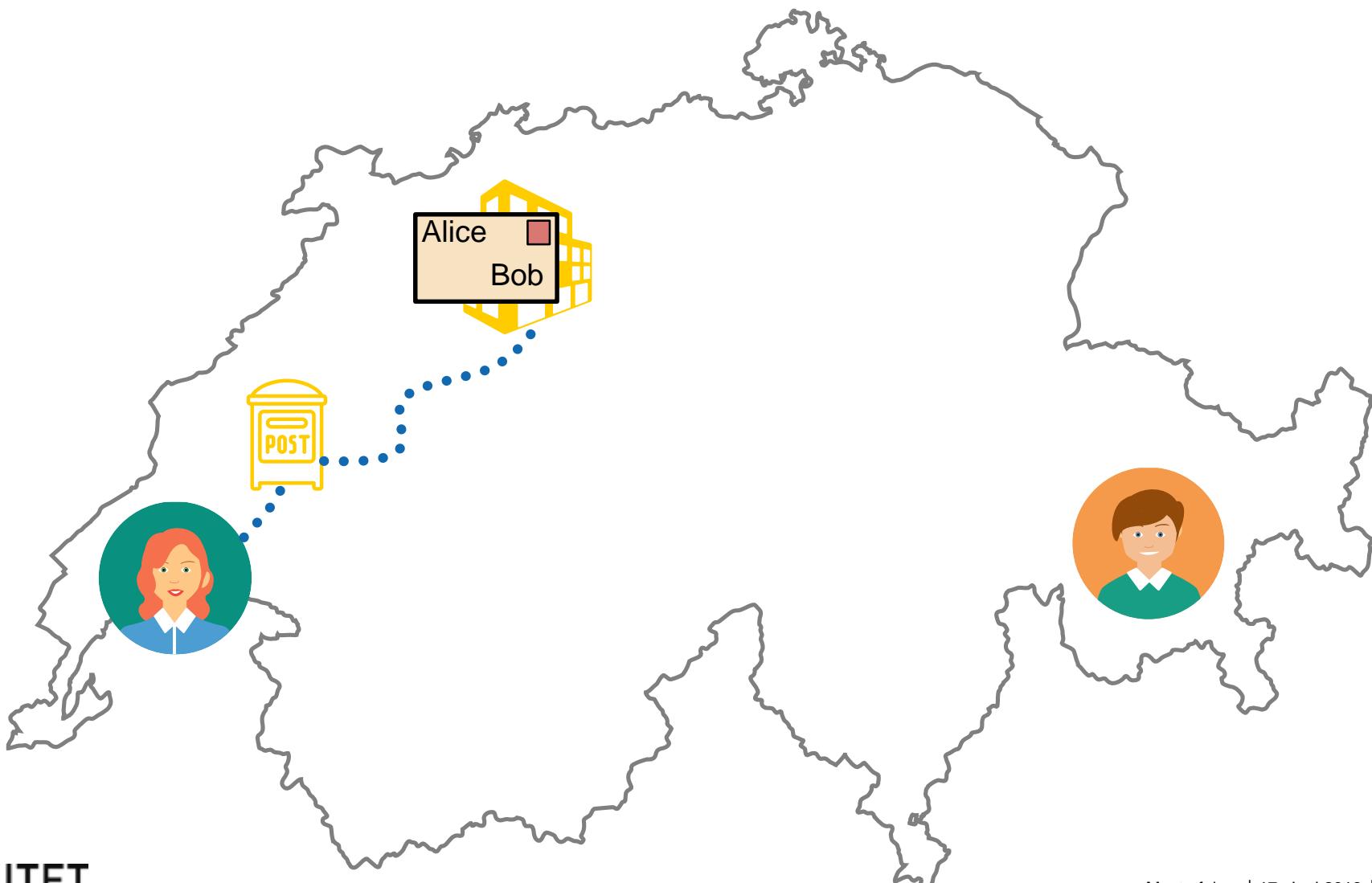
Alice writes a letter to Bob...



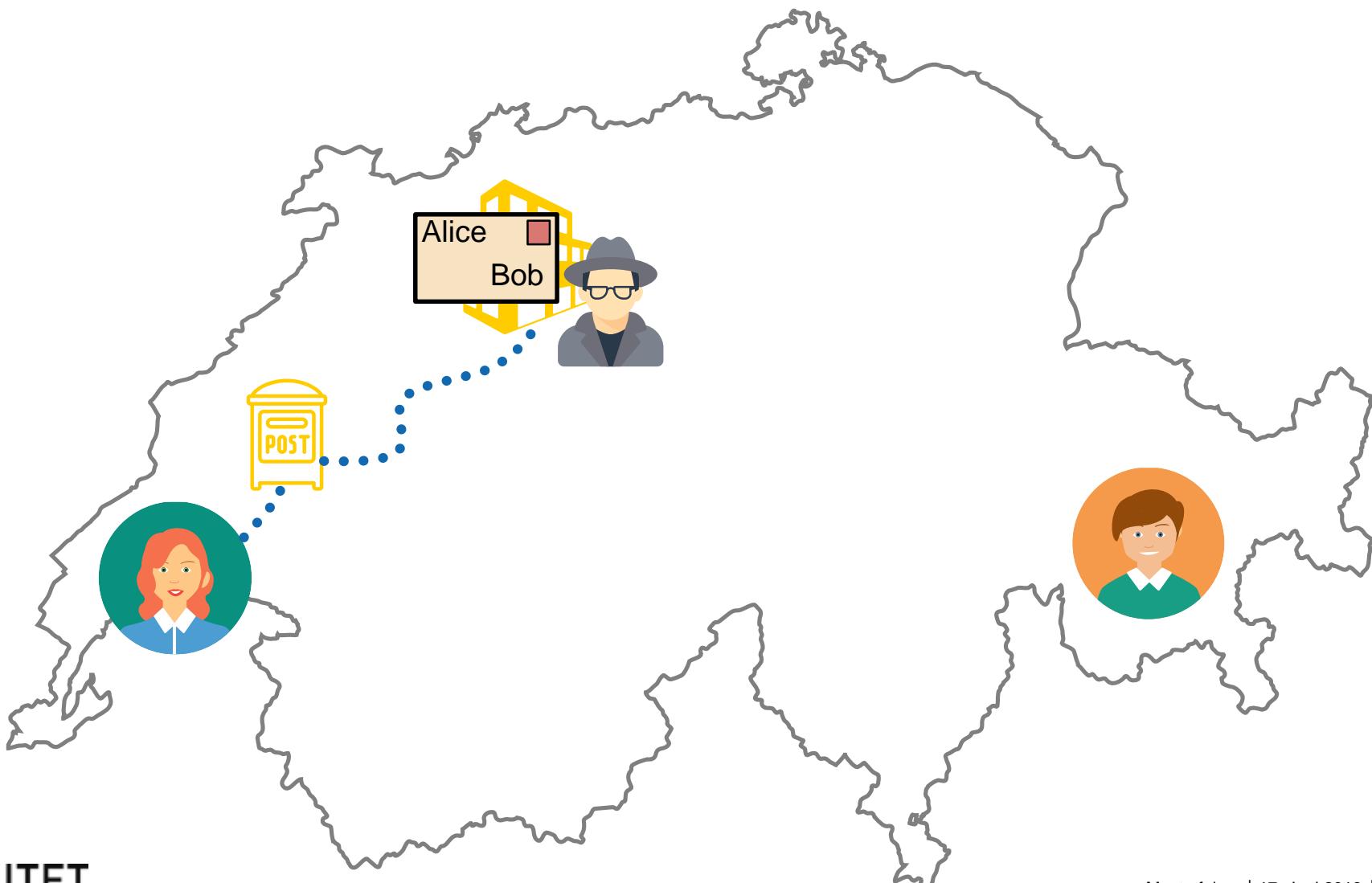
Alice writes a letter to Bob...



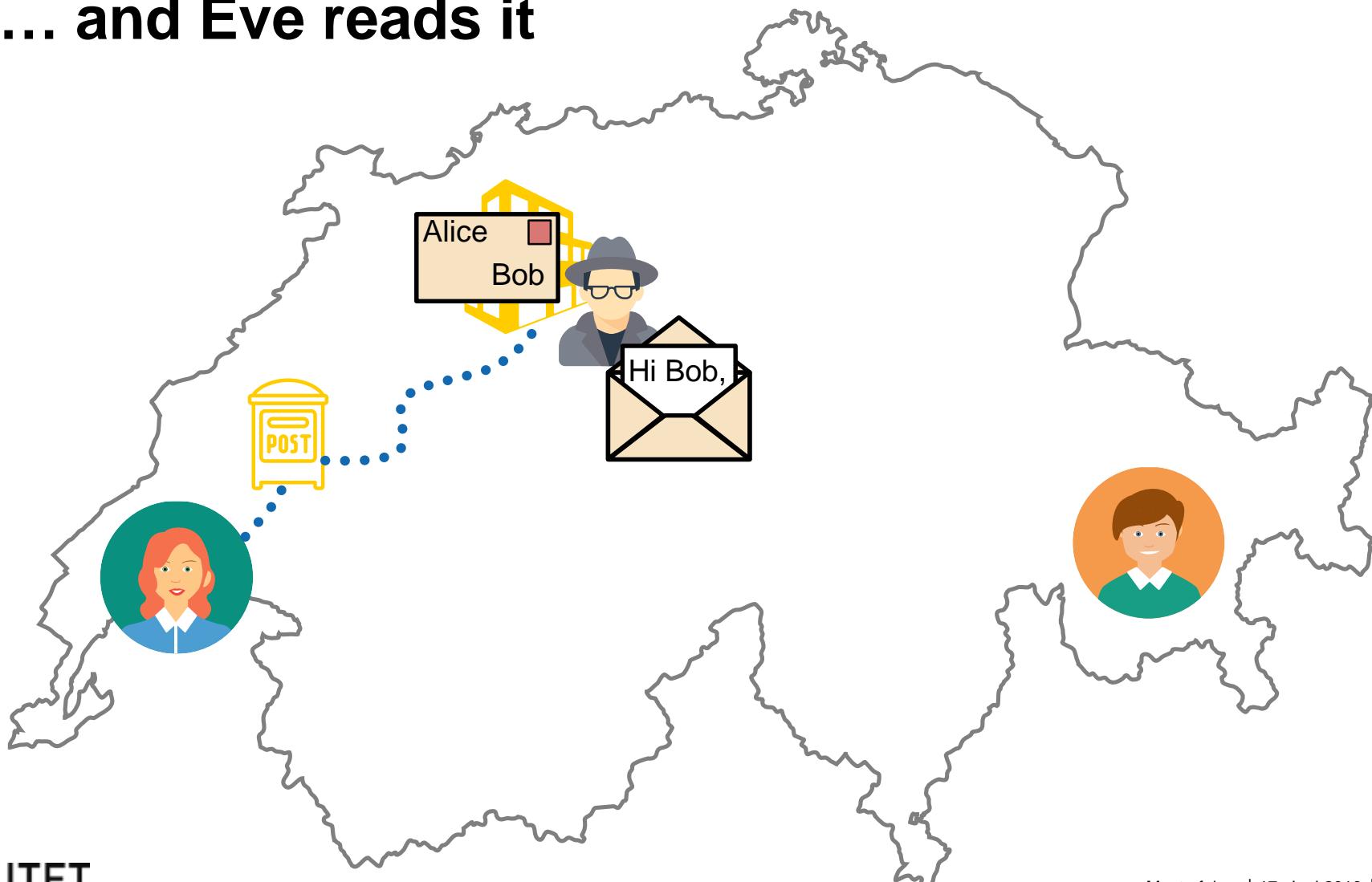
Alice writes a letter to Bob...



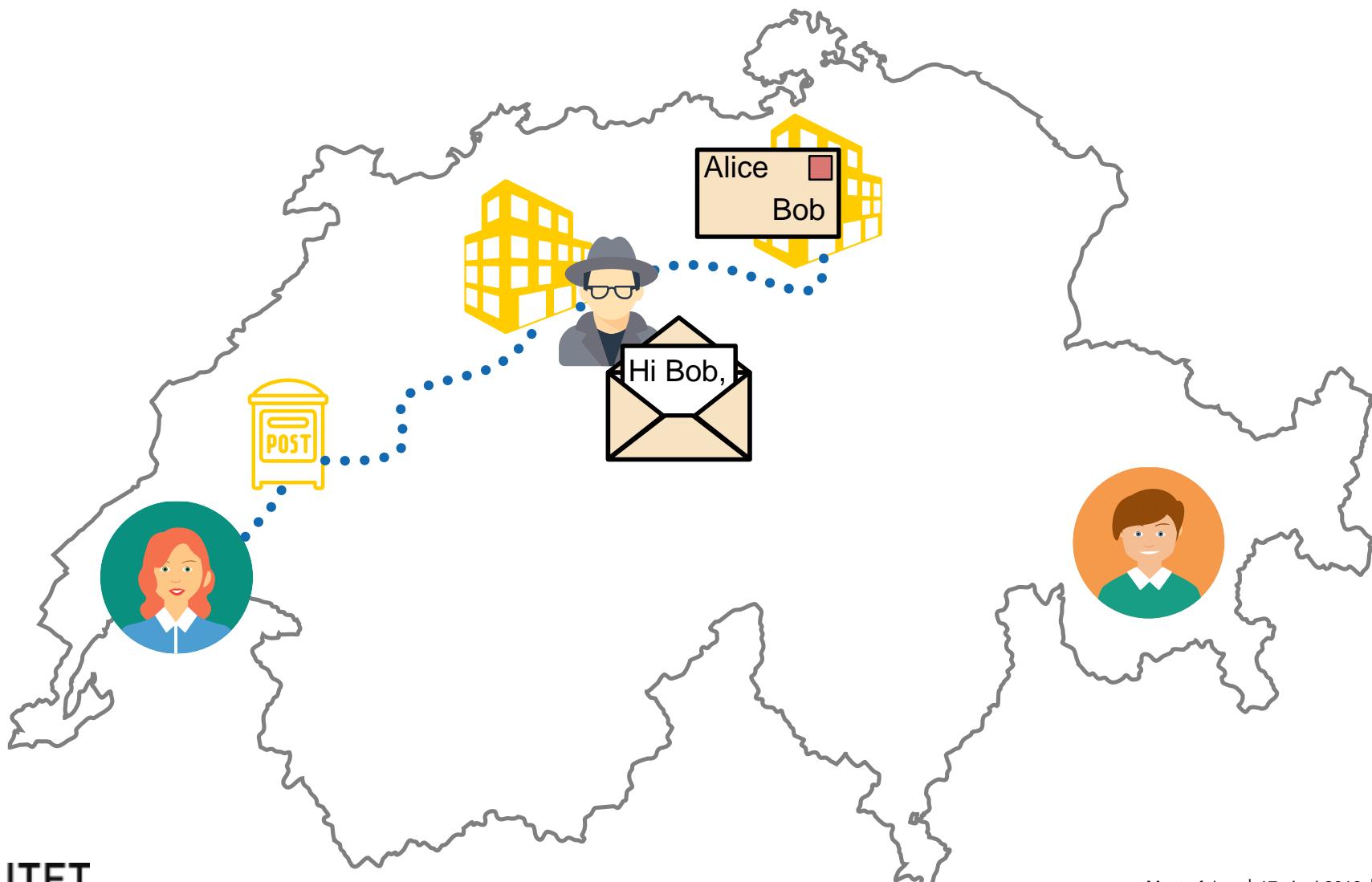
Alice writes a letter to Bob...



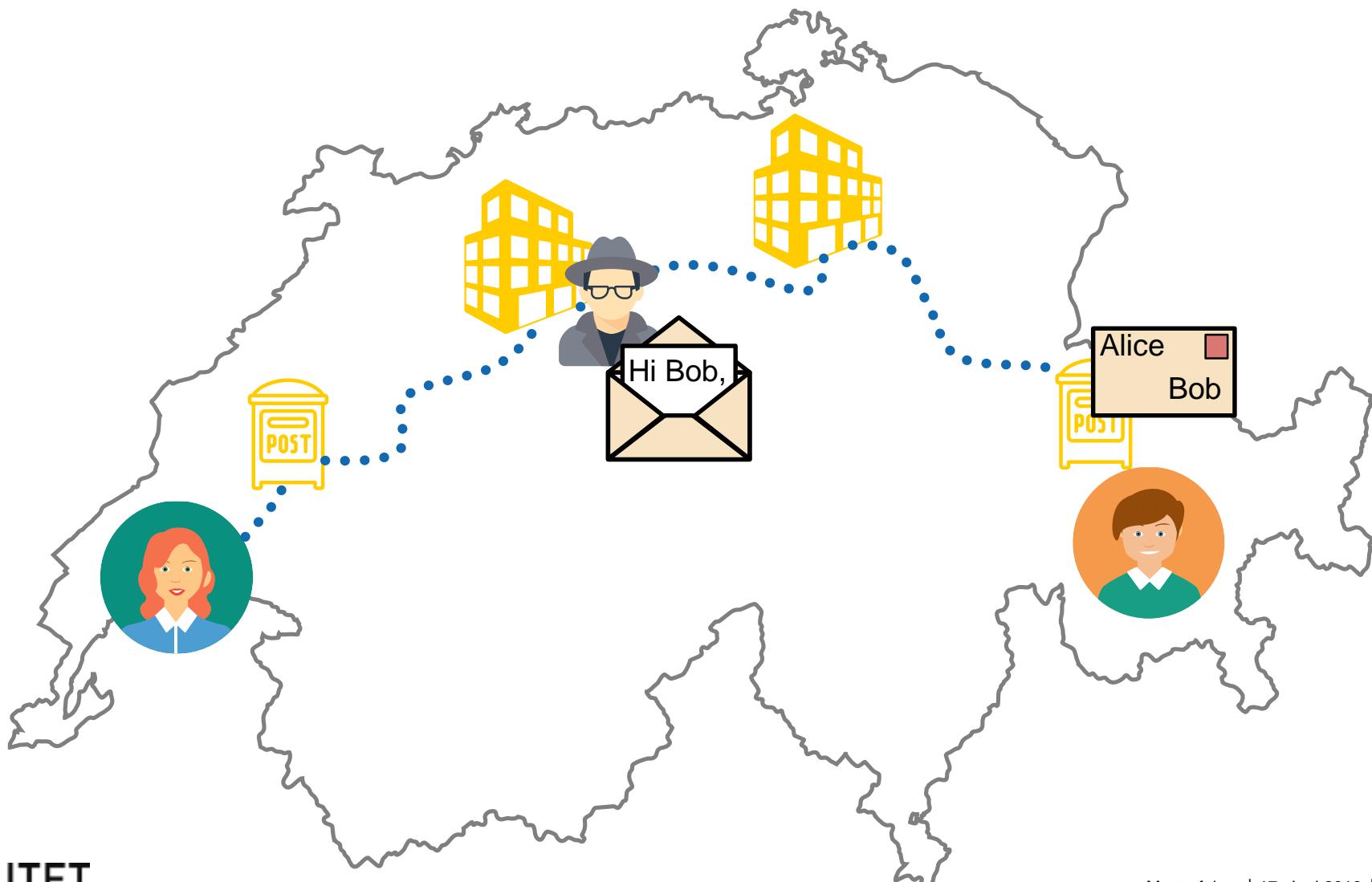
Alice writes a letter to Bob... ... and Eve reads it



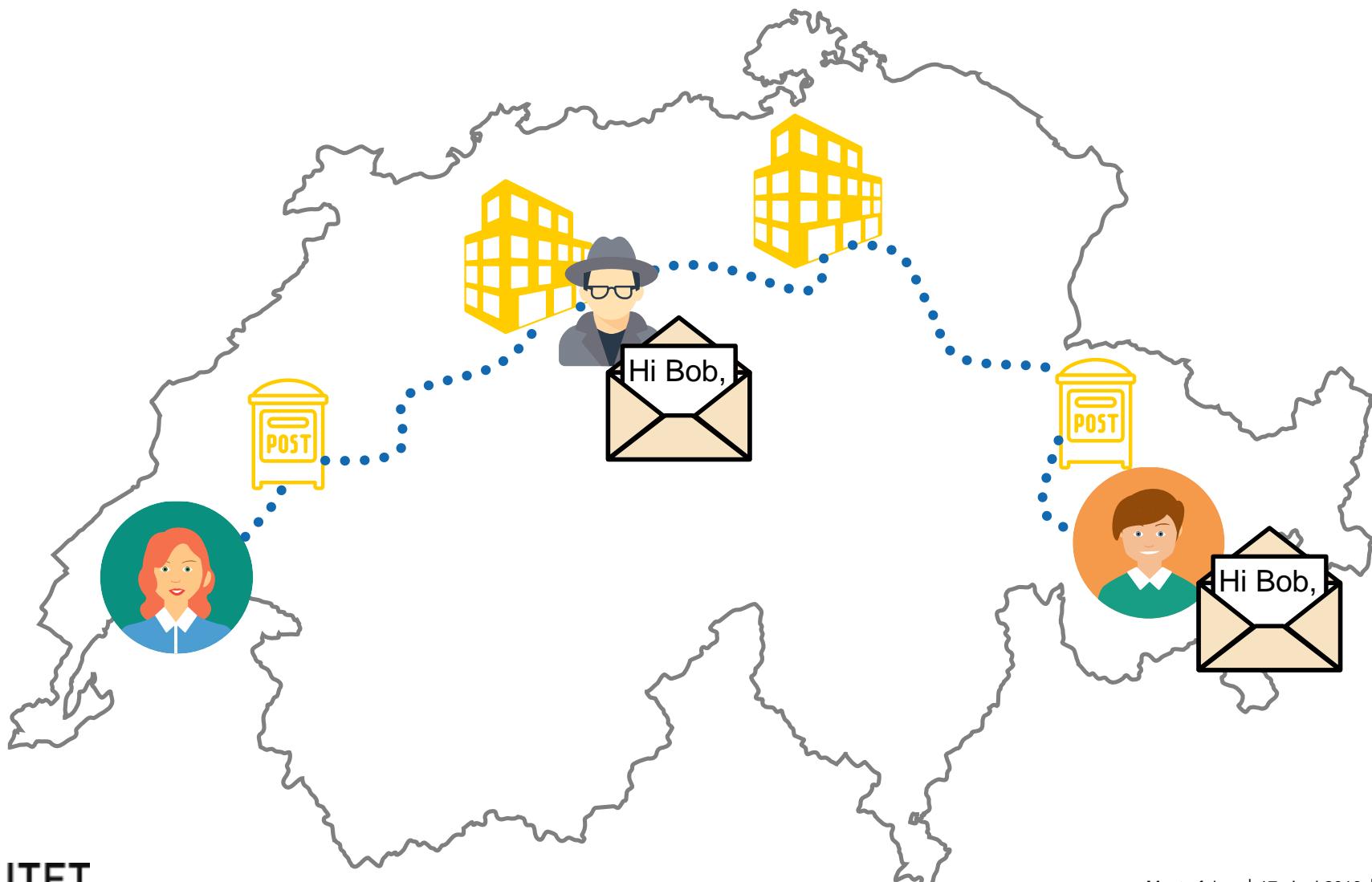
Alice writes a letter to Bob...



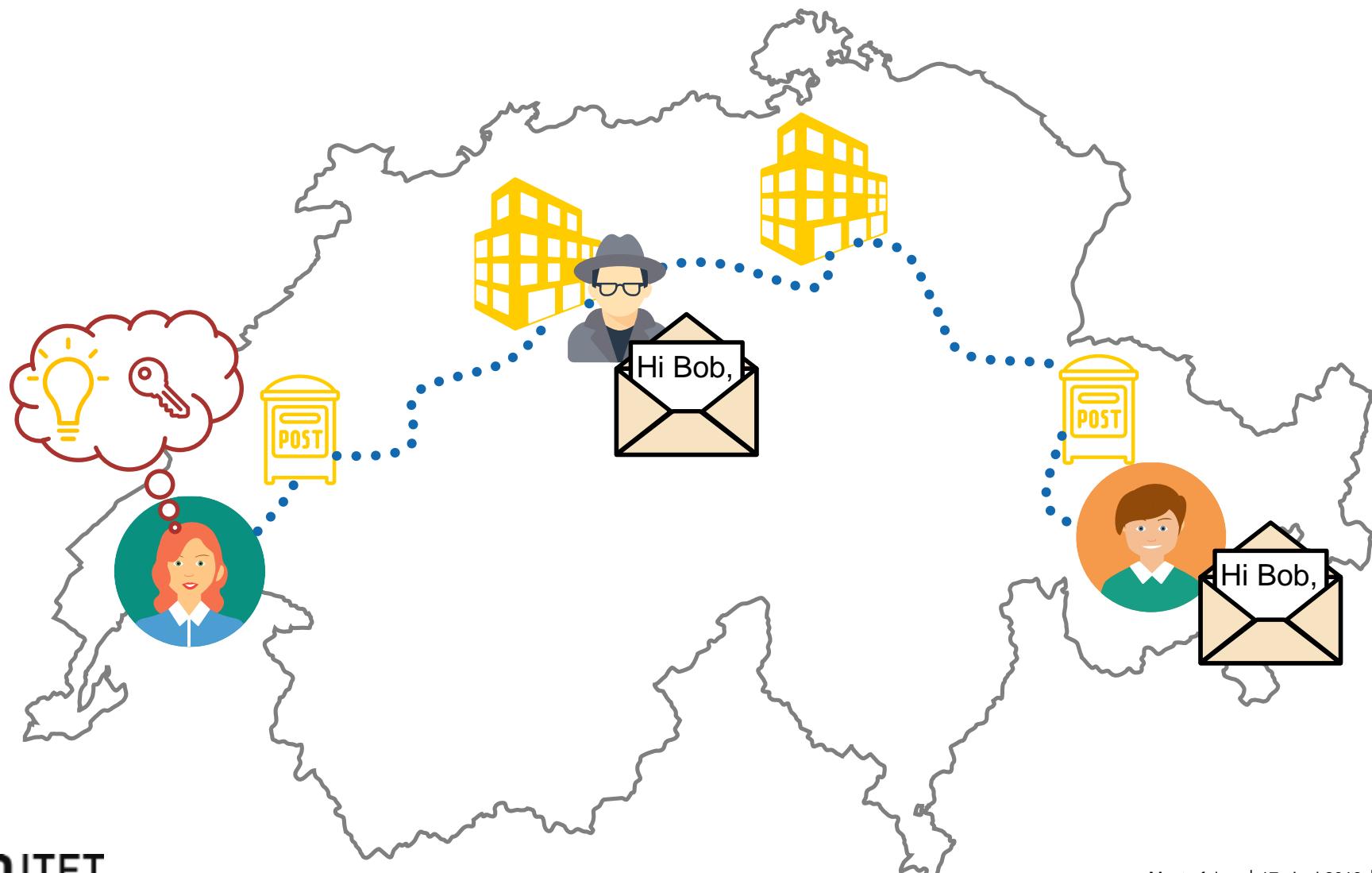
Alice writes a letter to Bob...



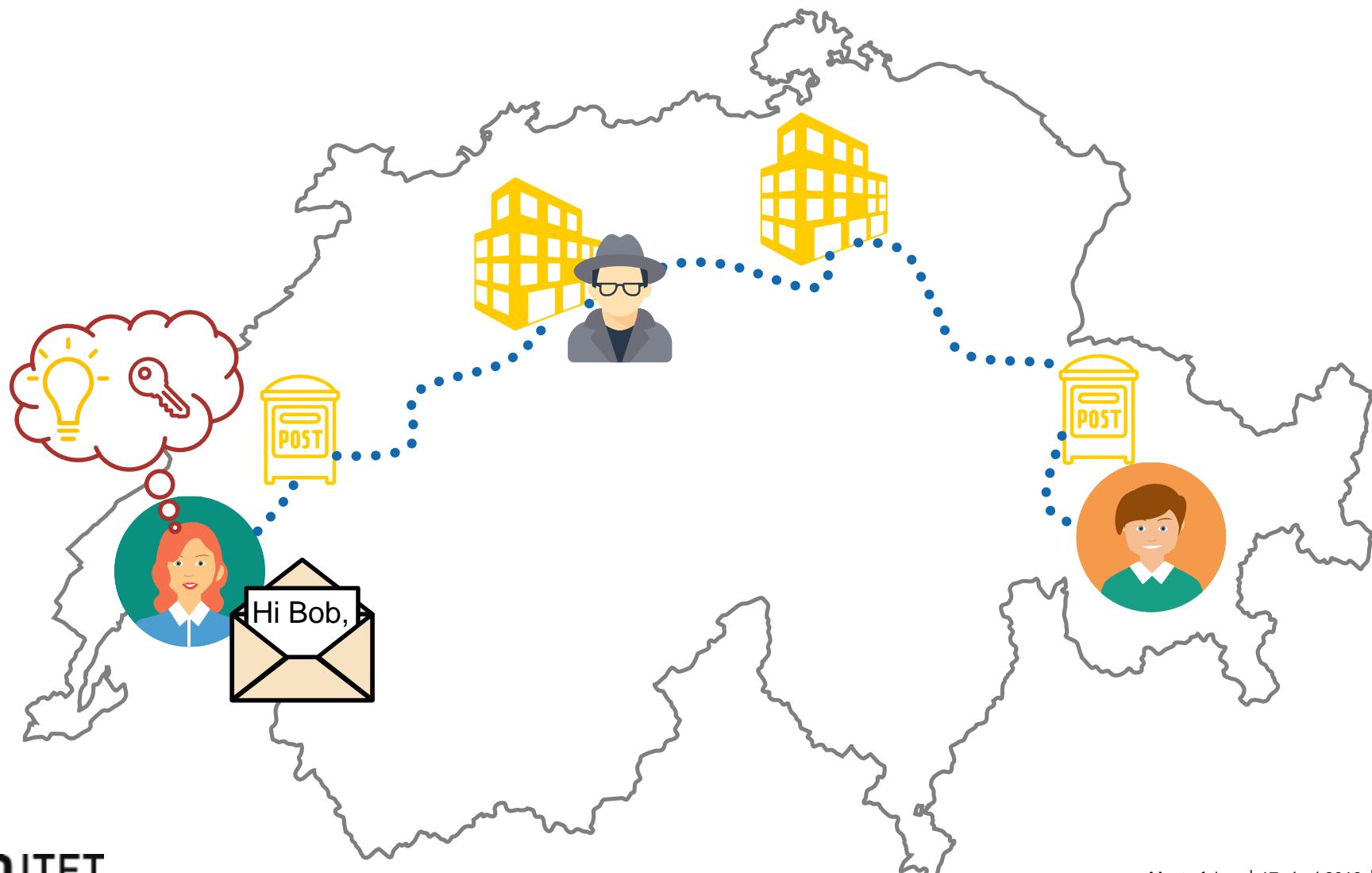
Alice writes a letter to Bob...



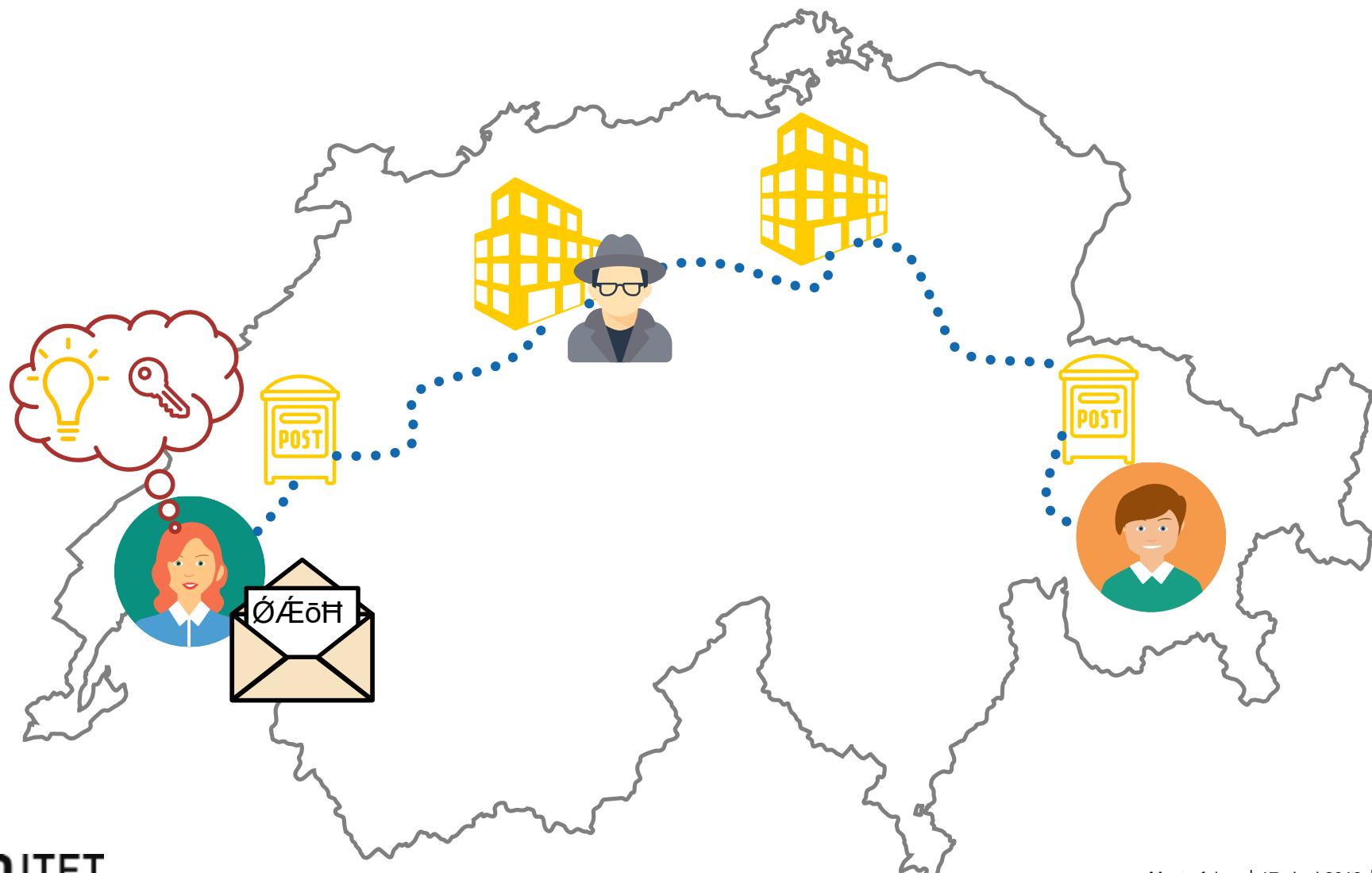
Alice encrypts the message...



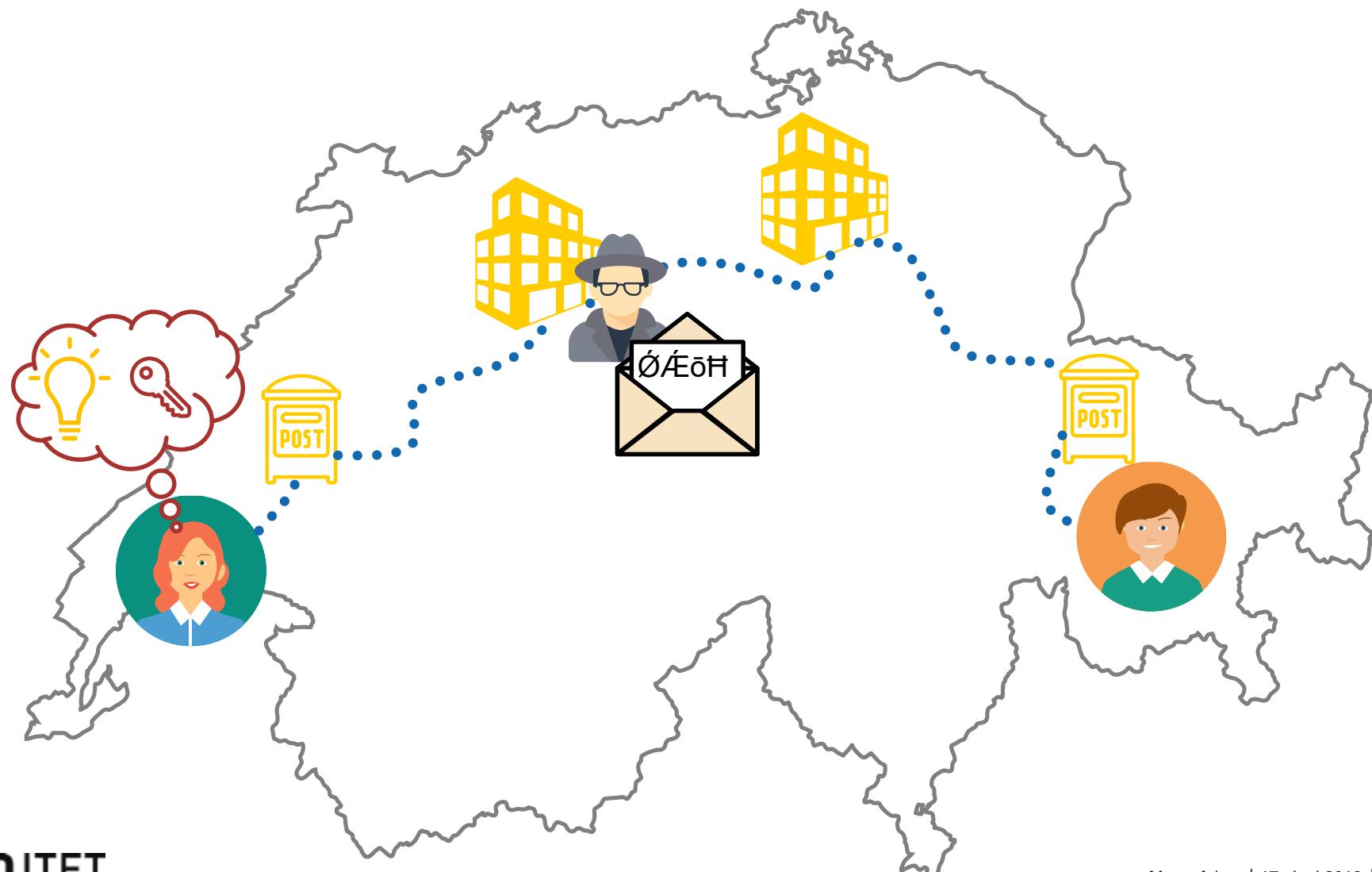
Alice encrypts the message...



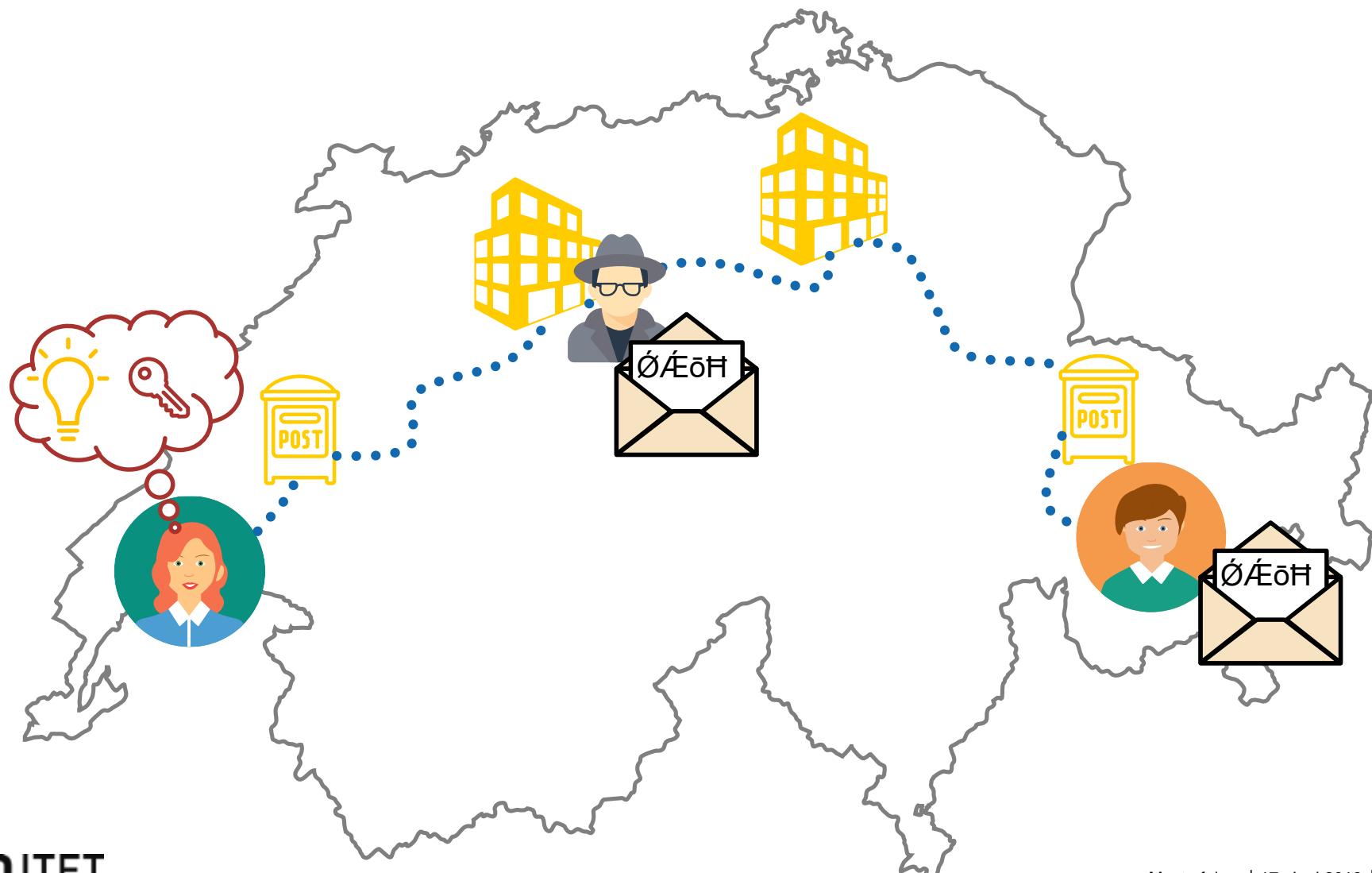
Alice encrypts the message...



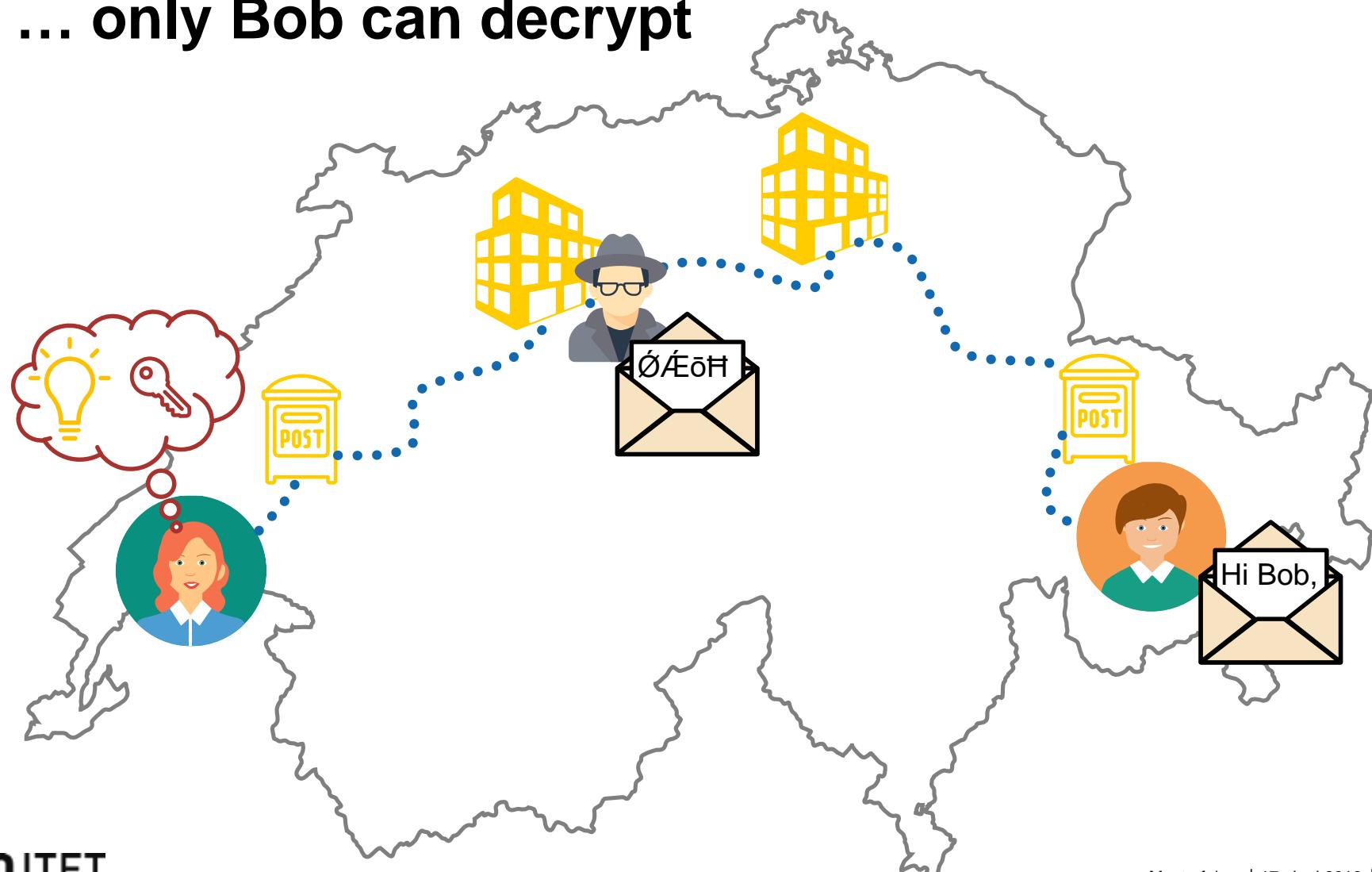
Alice encrypts the message...



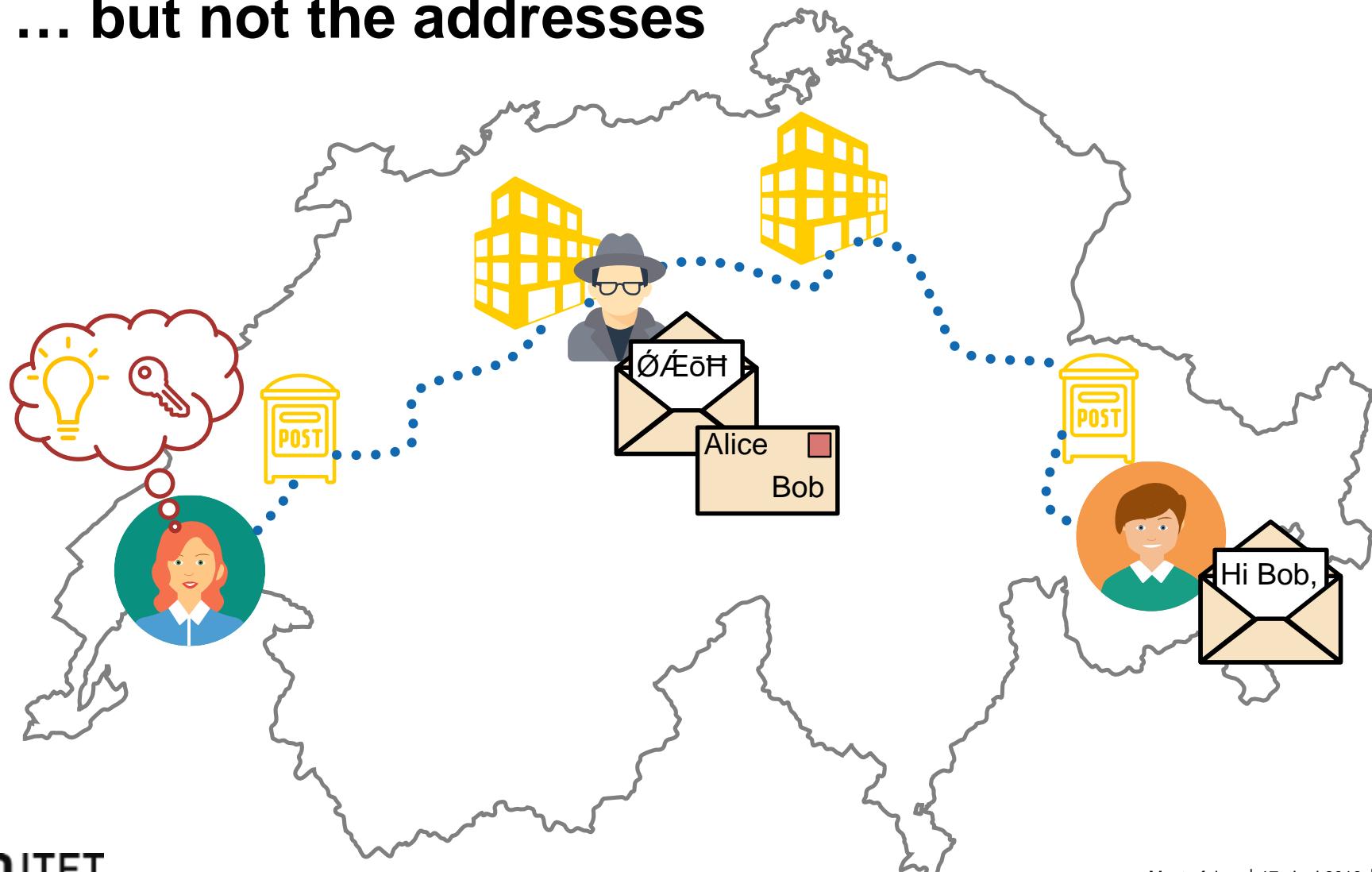
Alice encrypts the message...



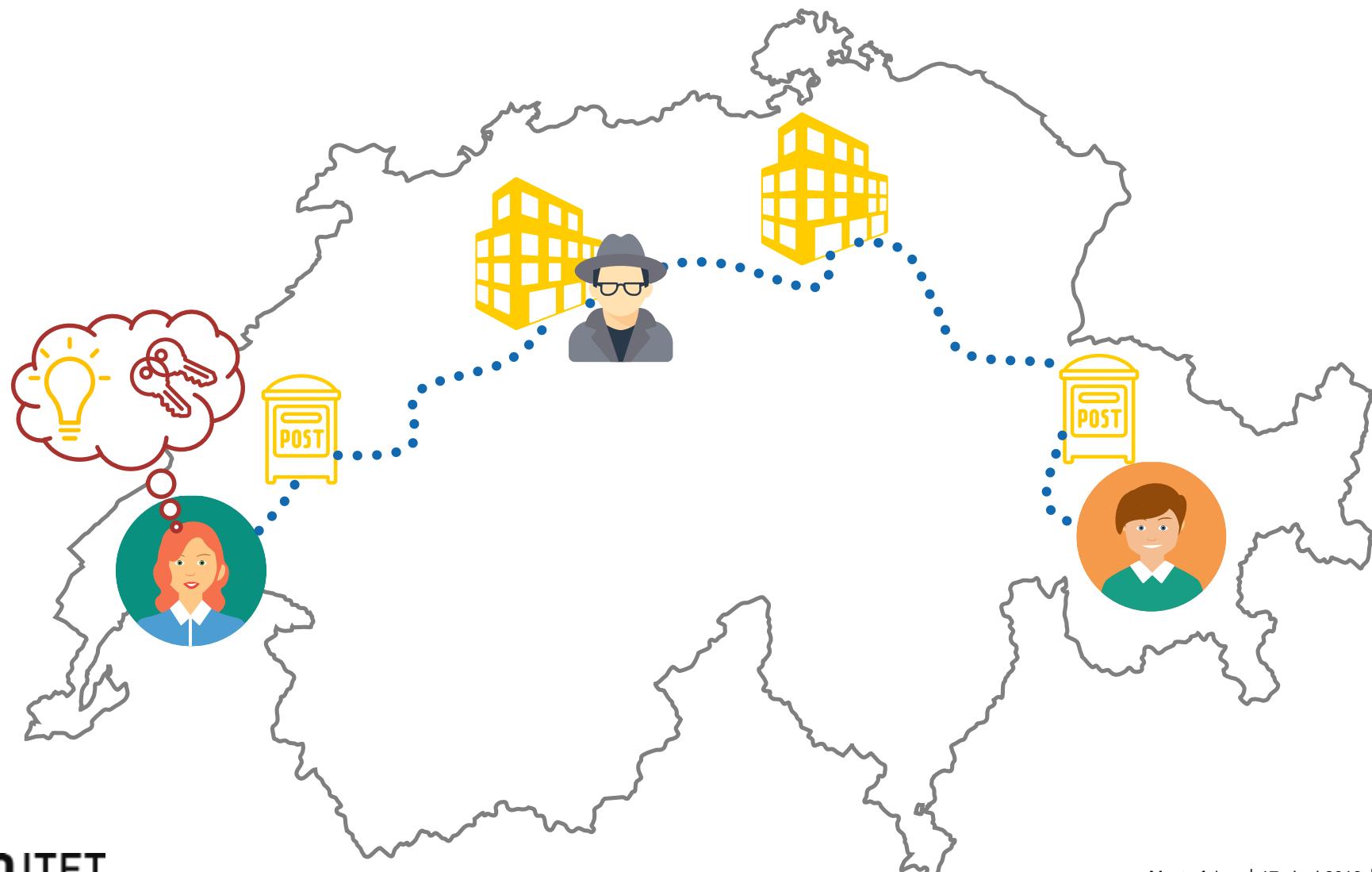
Alice encrypts the message...
... only Bob can decrypt



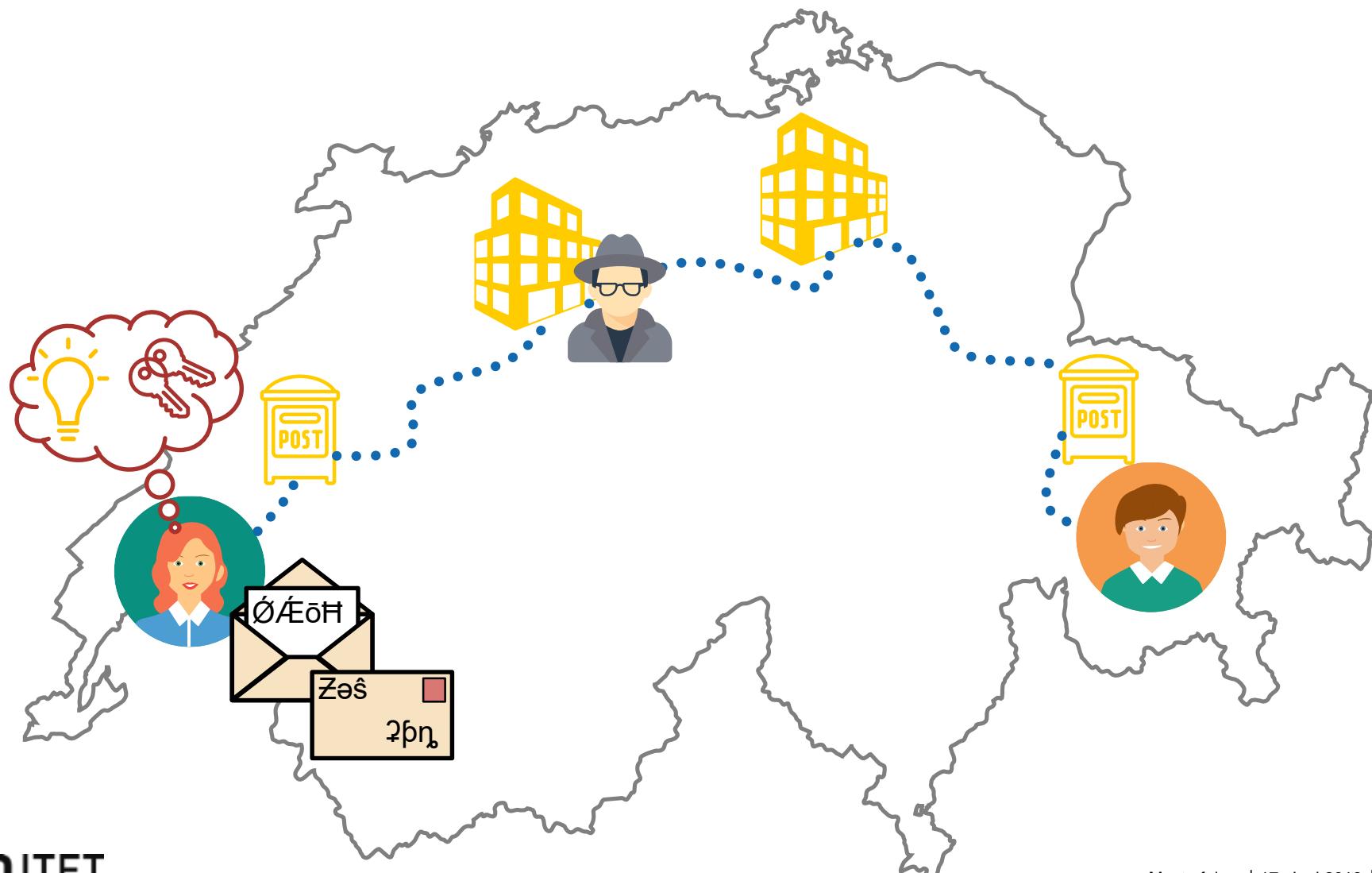
Alice encrypts the message... ... but not the addresses



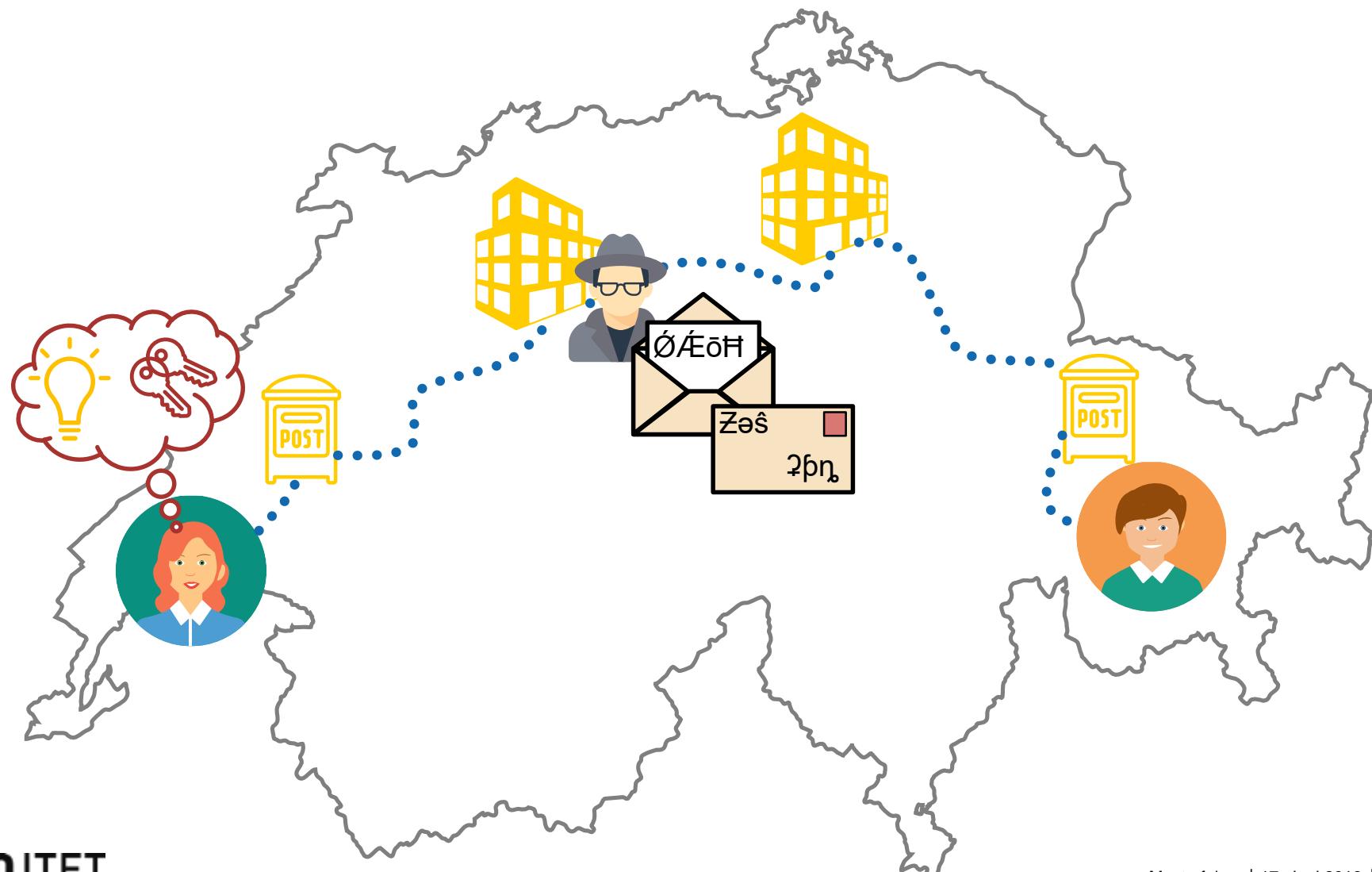
Alice encrypts the message & the addresses...



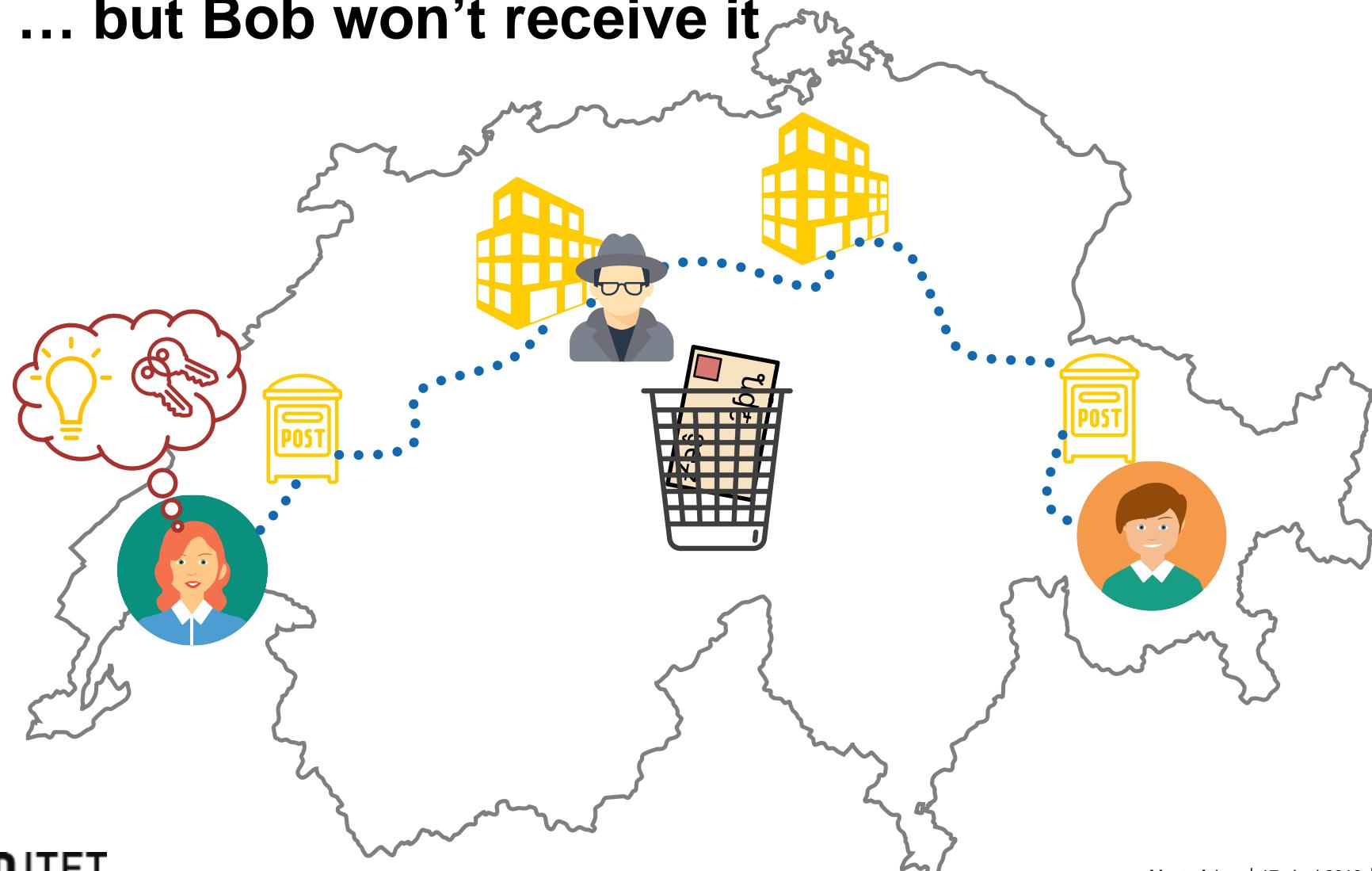
Alice encrypts the message & the addresses...



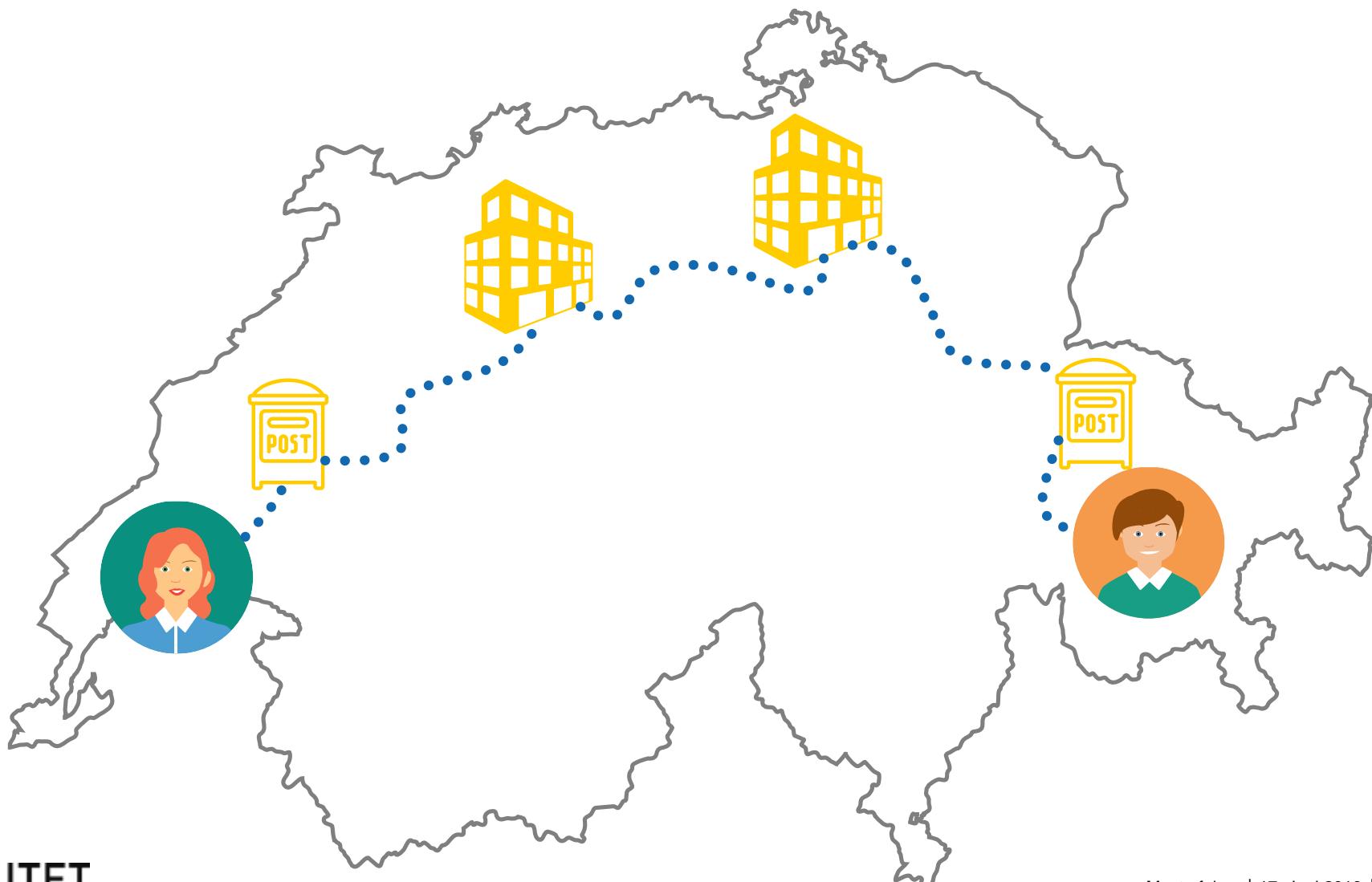
Alice encrypts the message & the addresses...



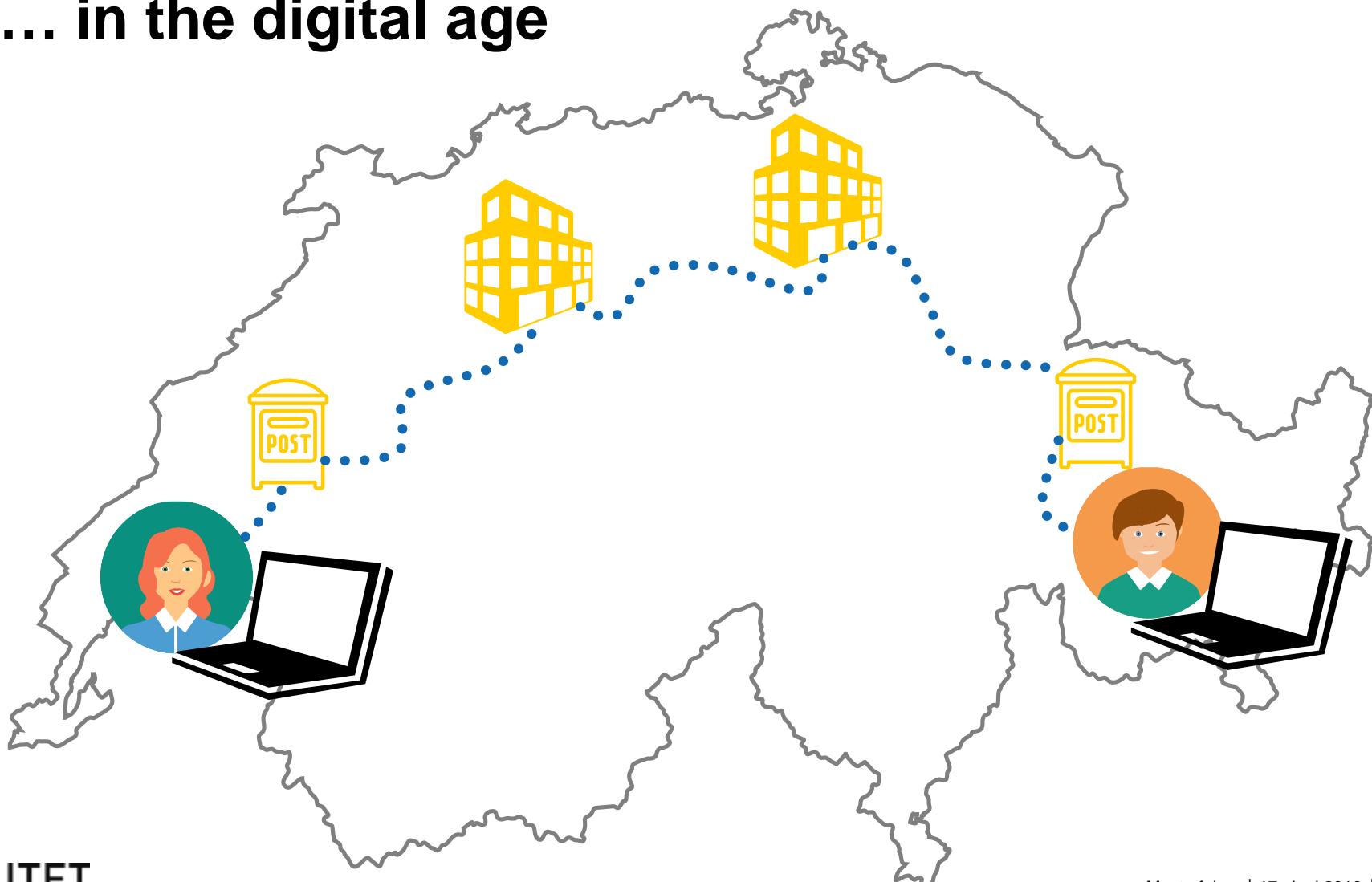
Alice encrypts the message & the addresses...
... but Bob won't receive it



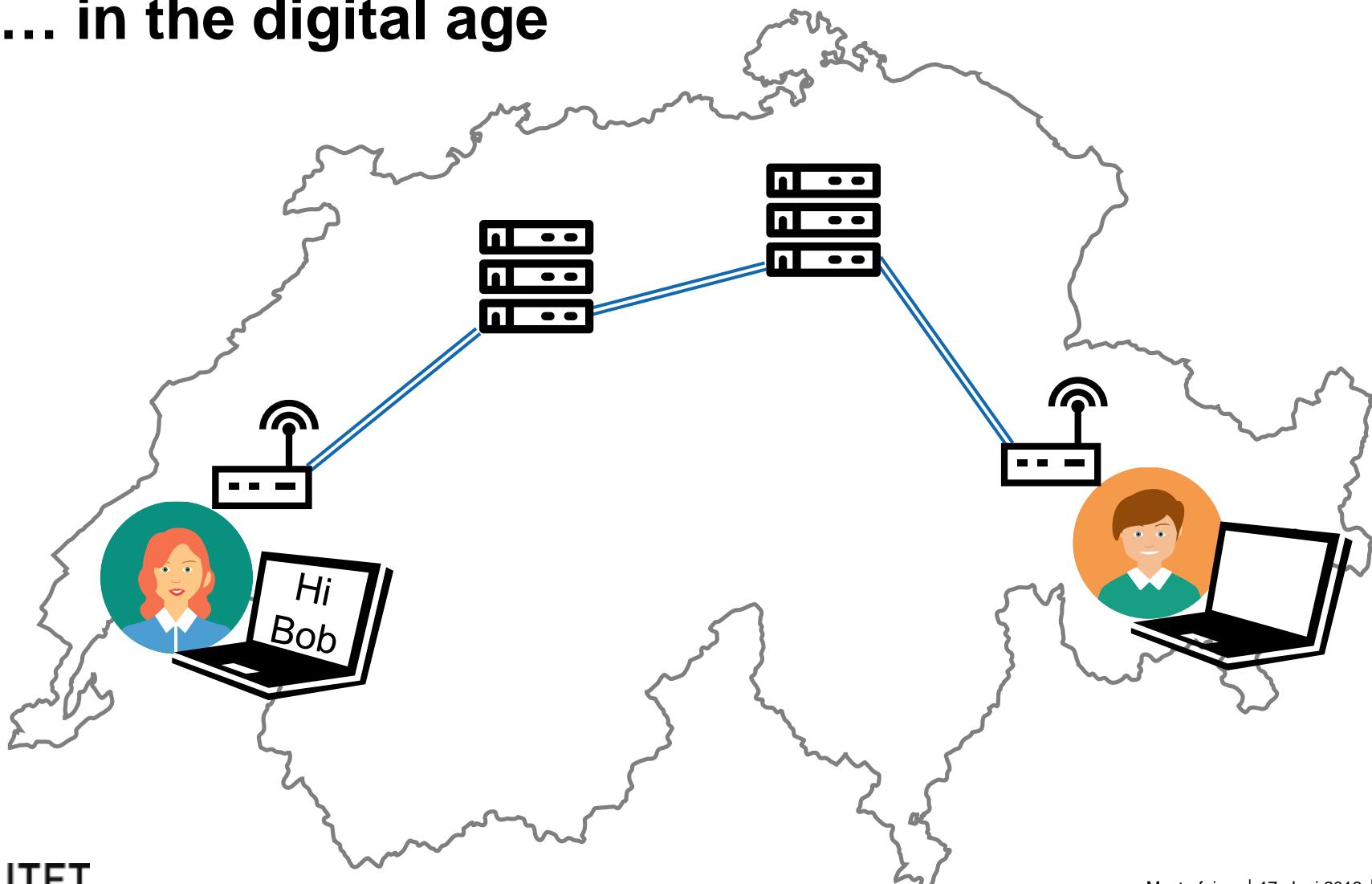
Alice writes a letter to Bob...



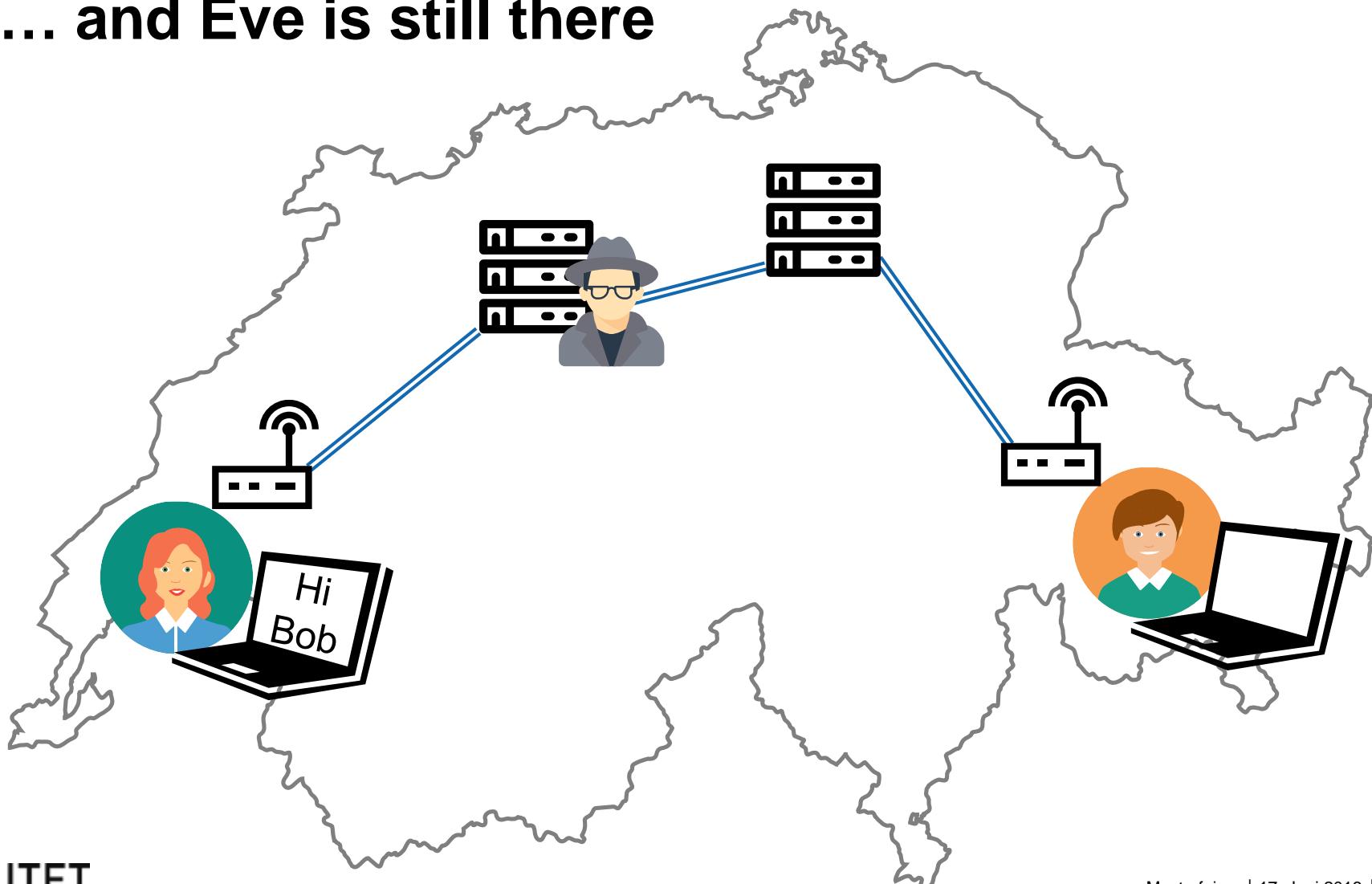
Alice writes a letter to Bob... ... in the digital age



Alice writes a letter to Bob... ... in the digital age



Alice writes a electronic letter to Bob... ... and Eve is still there

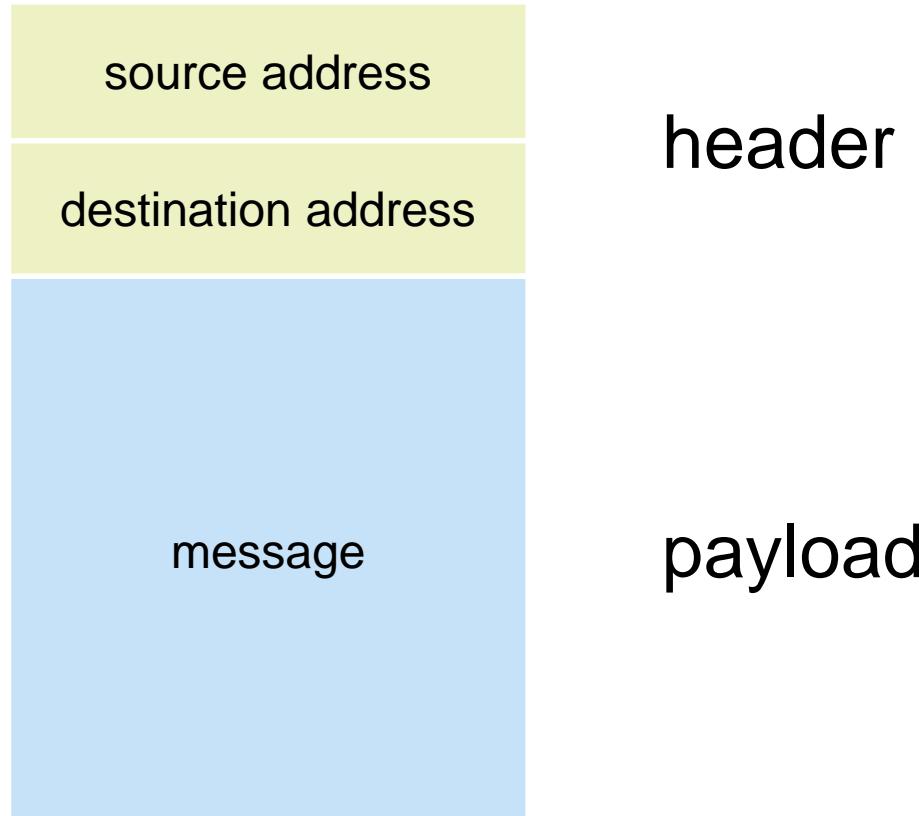


Packets are the letters in computer networks

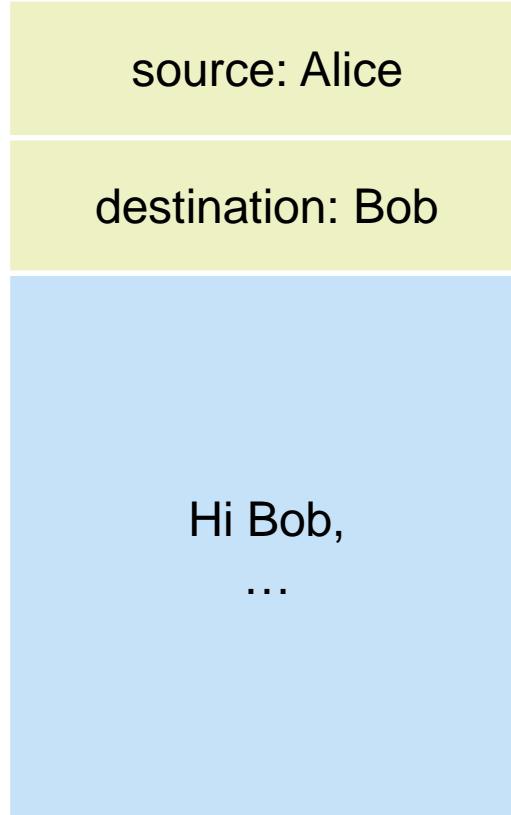


packet

Packets consist of headers and payloads



Packets consist of headers and payloads



header

payload

Existing solutions only protect the payload



Payload encryption
SSL/TLS, IPsec, MACsec



Metadata obfuscation
No existing solution

Network obfuscation by rewriting addresses

What?

Rewrite source and destination addresses
MAC, IP, TCP/UDP port

Where?

At ingress and egress switch
Agnostic for end-hosts

Network obfuscation by rewriting addresses

What?

Rewrite source and destination addresses
MAC, IP, TCP/UDP port

Where?

At ingress and egress switch
Agnostic for end-hosts

Challenge

Scalability
Anonymity vs. scalability

Network obfuscation can provide multiple kinds of anonymity

Communication anonymity

Who is talking to whom?

Volume anonymity

How often are A and B talking to each other?

Topology anonymity

How many clients are in the network?

SDN-based Network Obfuscation

SDN-based Network Obfuscation

SDN-based Network Obfuscation

Software-Defined Network

Networking infrastructure before SDN



closed software

closed hardware

[Cisco]

Networking infrastructure before SDN

after SDN



closed software

[Cisco]

closed hardware

open software



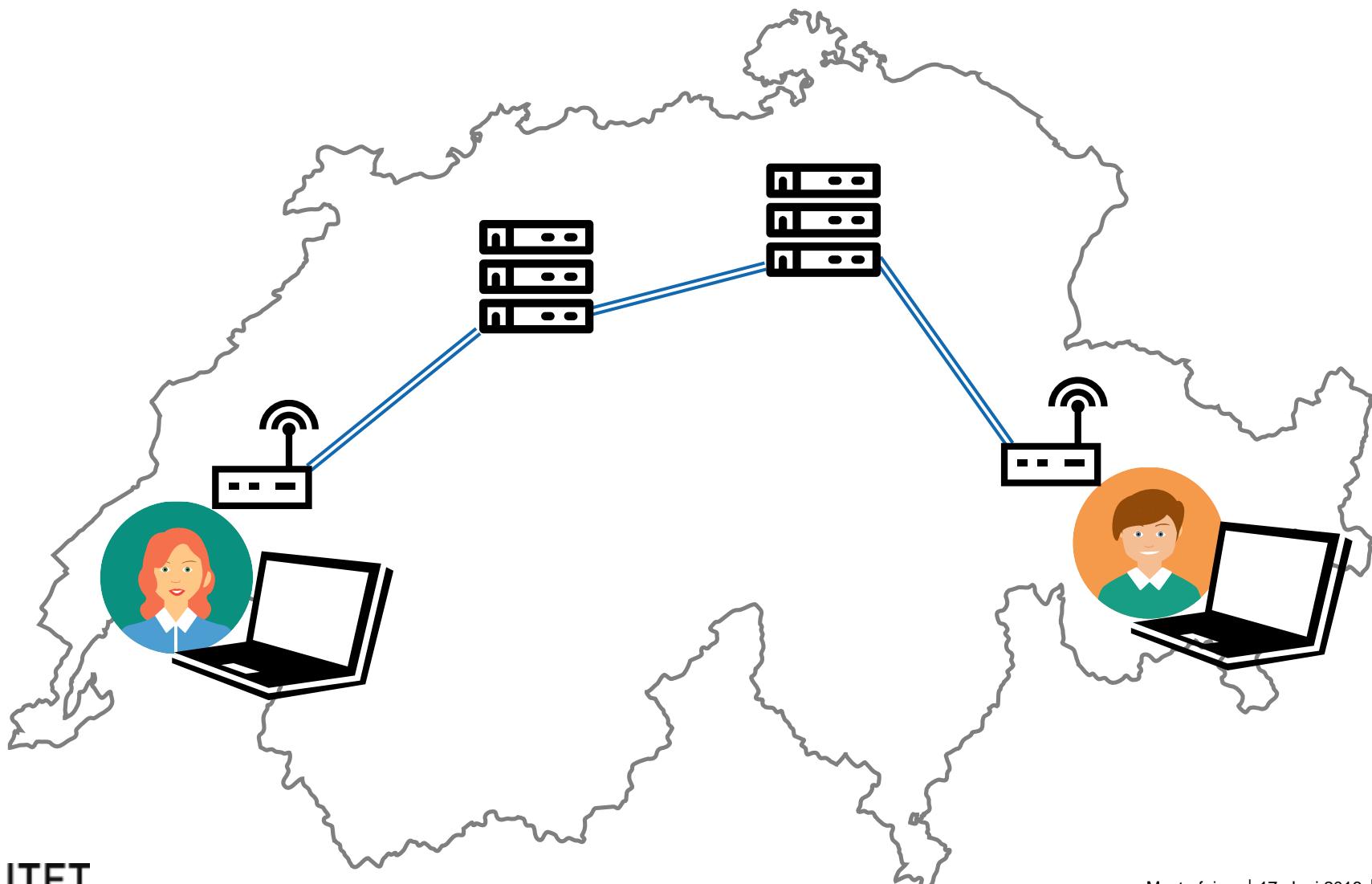
standardized interface

standardized hardware

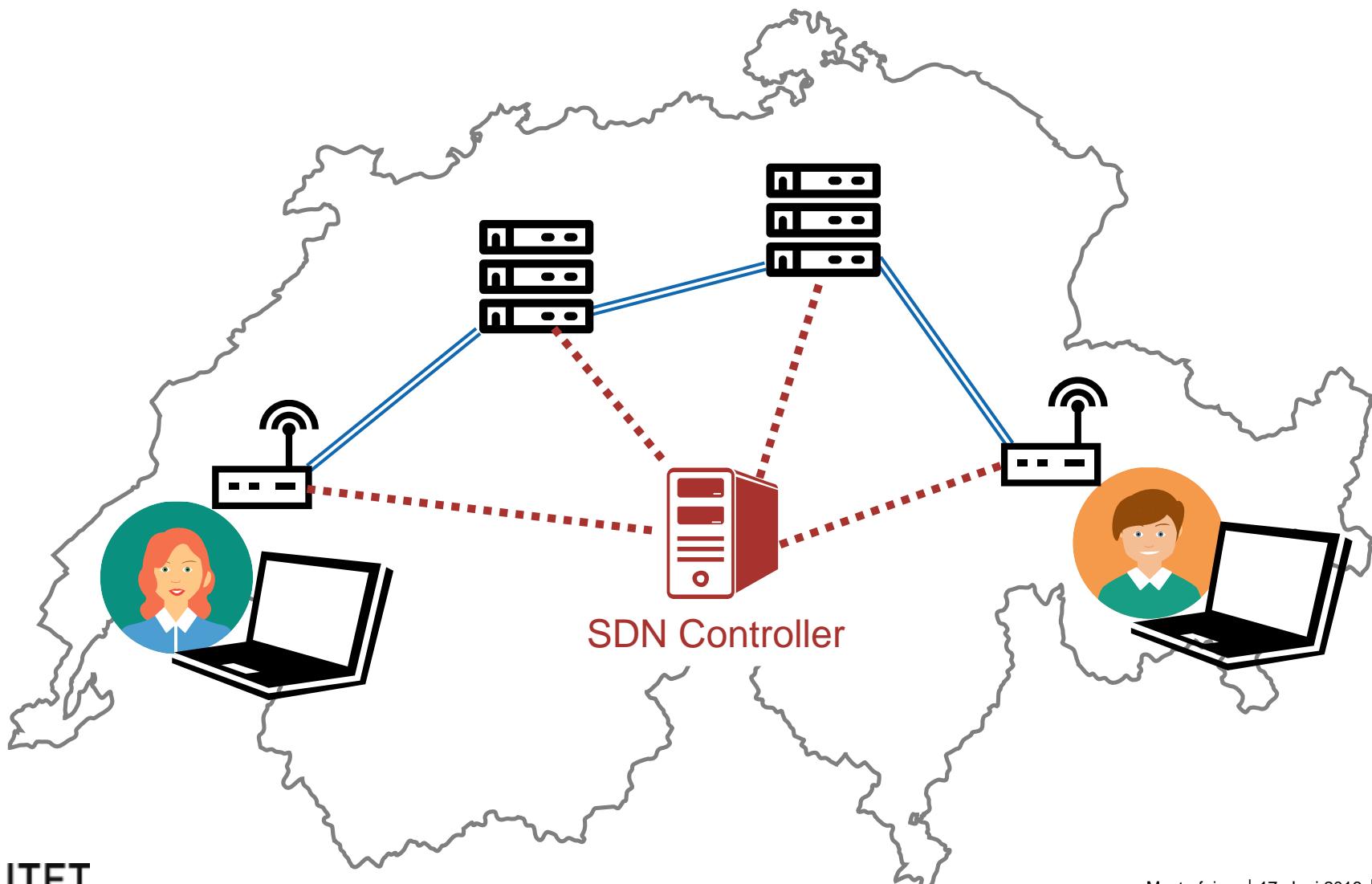


[HP]

Software-Defined Networks



Software-Defined Networks: Central controller



SDN-based Network Obfuscation

Master Thesis
Roland Meier

Thanks for your attention