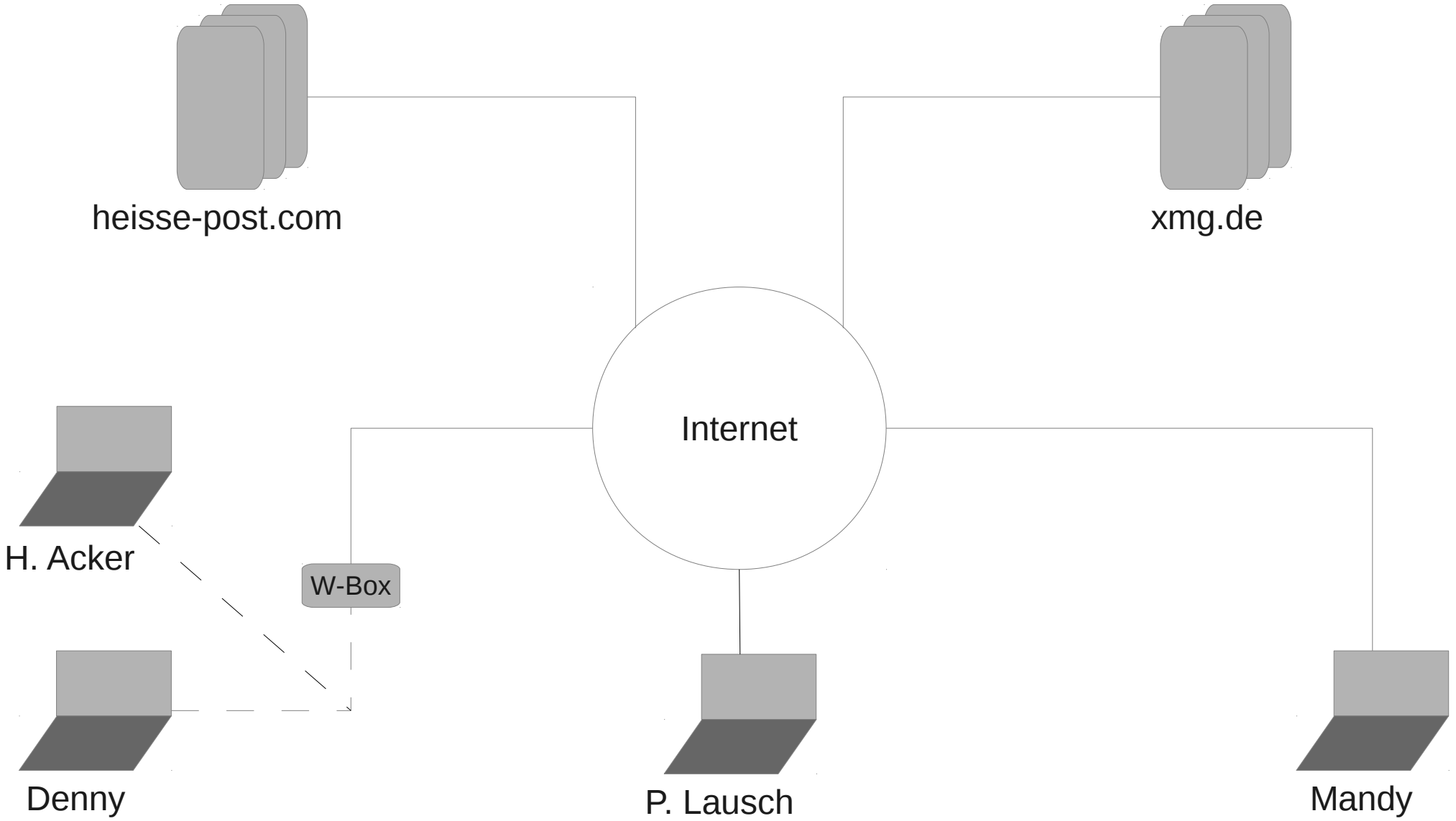
Yes we can – monitor you

Martin Christian und Christian Perle

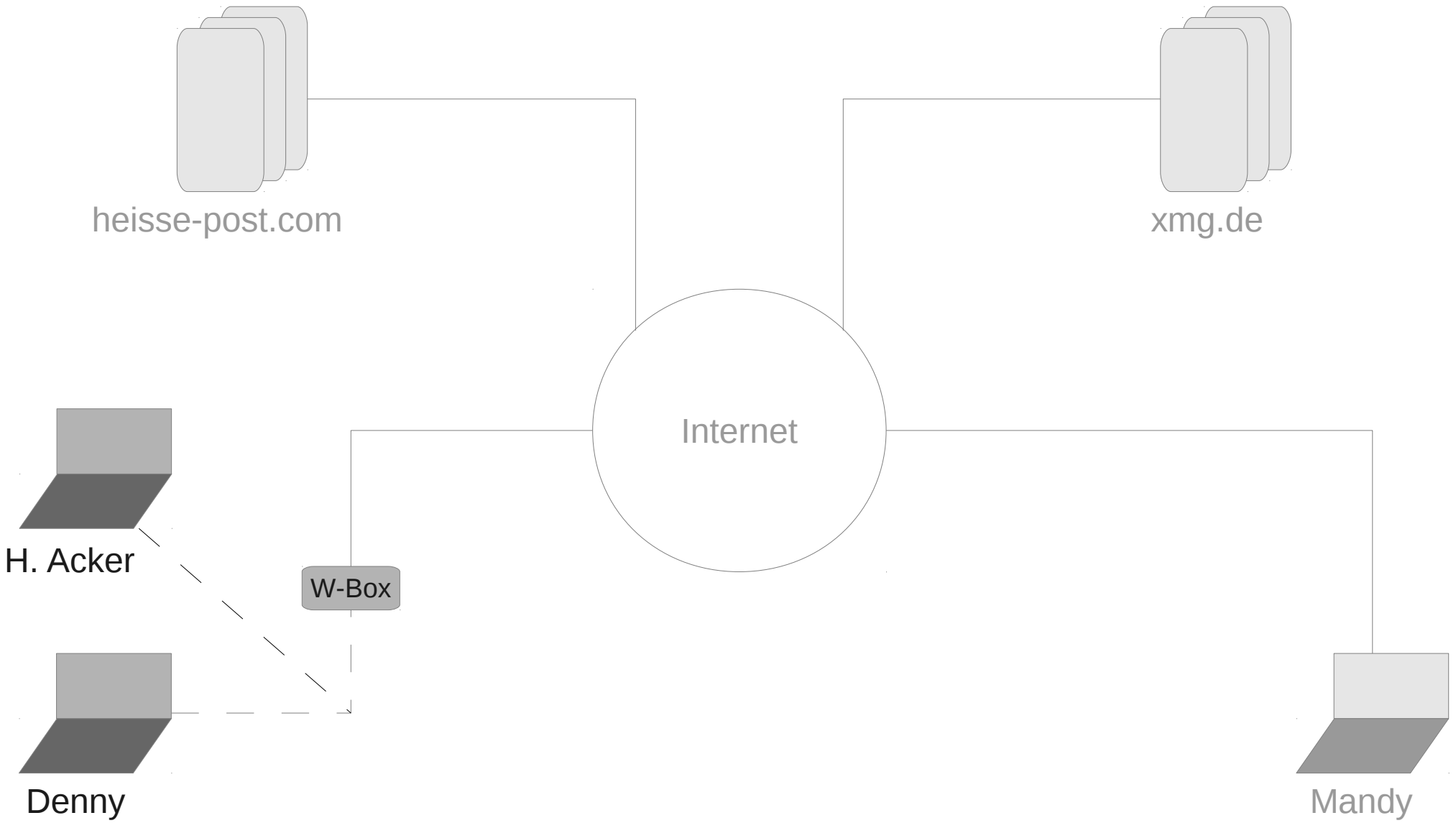
Gliederung

- Szenario
- Szene 1: WLAN absichern
- Grundlagen
- Hops (Hopser)
- Szene 2: Webzugriffe absichern
- Szene 3: Vorsicht bei Zertifikaten
- Szene 4: Providersicherheit
- Szene 5: Lokalen Abruf von Mails absichern
- Pretty Good Privacy®
- Szene 6: Ende-zu-Ende Verschlüsselung
- Tools

Szenario


heisse-post.com
xmg.de
Internet
H. Acker
W-Box
Denny
P. Lausch
Mandy

WLAN absichern



Abhören im Internet

Grundlagen

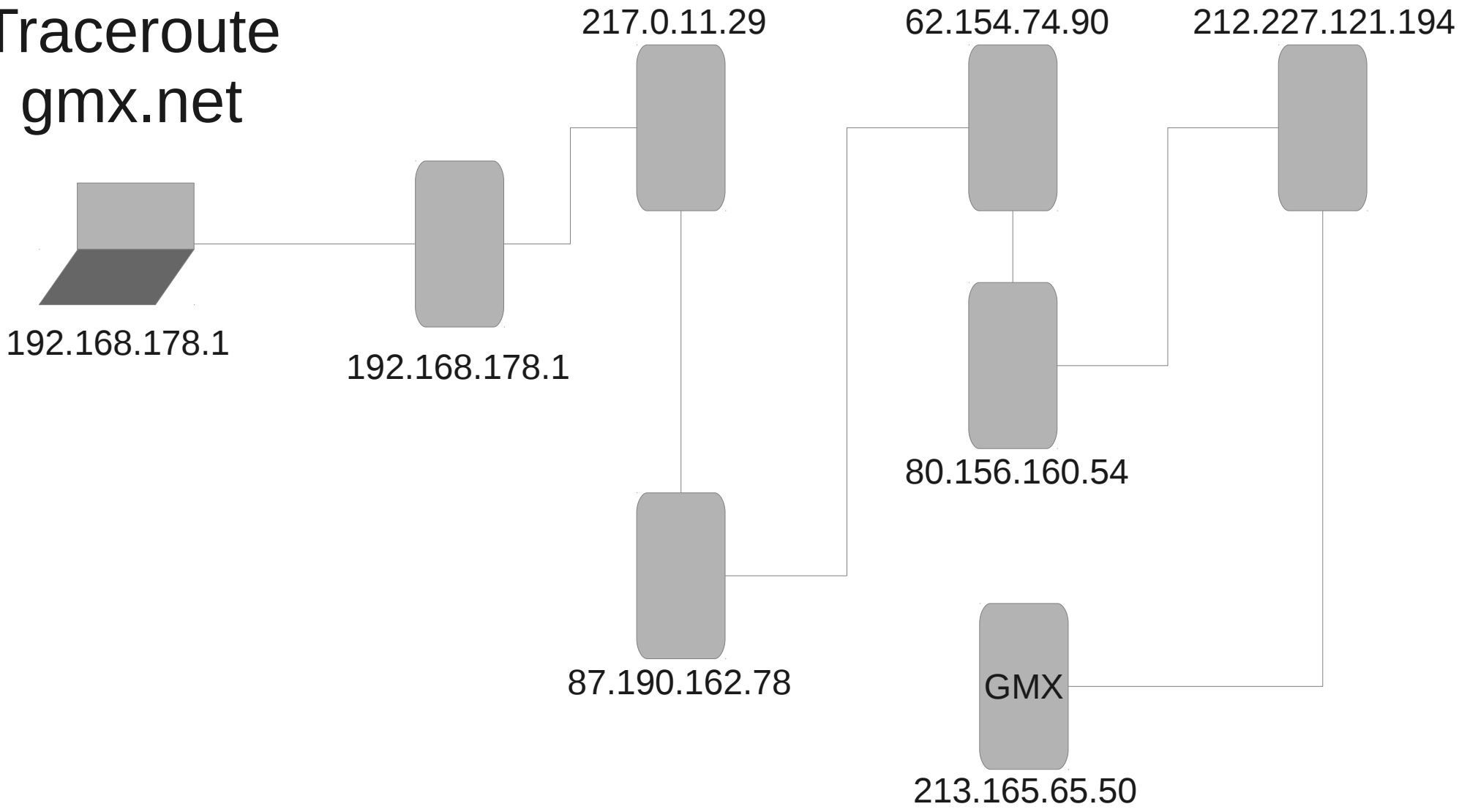
Anwendungen	Hypertext Transfer Protocol	GET heisse-post.com/
Transport	Transmission Control Protocol	Port Nr. 80 Paket Nr. 3
Internet	Internet Protocol	Von: 192.168.178.34 An: 172.18.0.10
Netzzugang	Ethernet	Von: 52:54:00:12:34:51 An: 52:54:00:12:34:59

Grundlagen

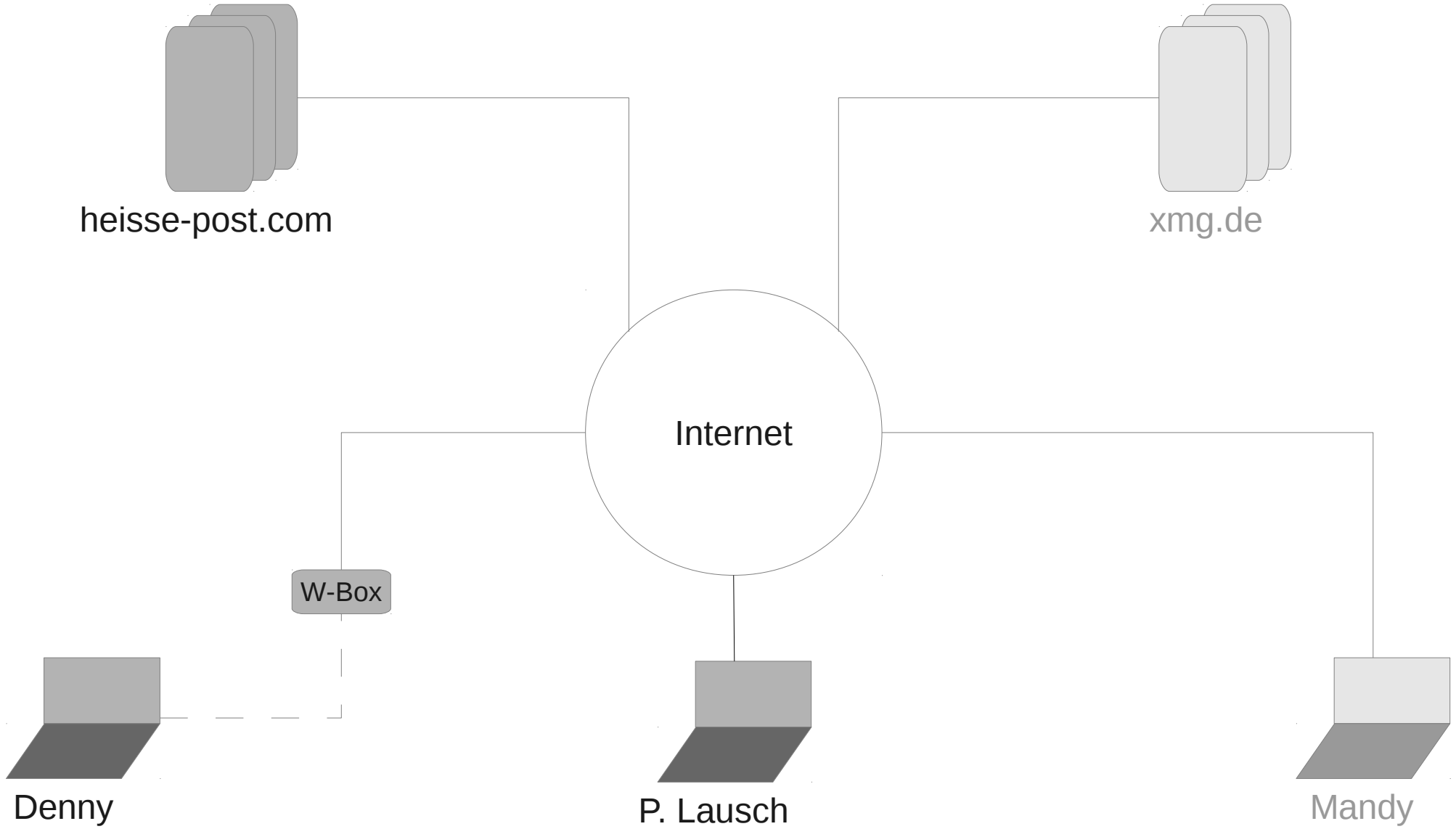
Ethernet	Internet Protocol	Transmission Control Protocol	Hypertext Transfer Protocol
			GET heisse-post.com/
		Port Nr. 80 Paket Nr. 3	GET heisse-post.com/
	Von: 192.168.178.34 An: 172.18.0.10	Port Nr. 80 Paket Nr. 3	GET heisse-post.com/
Von: 52:54:00:12:34:51 An: 52:54:00:12:34:59	Von: 192.168.178.34 An: 172.18.0.10	Port Nr. 80 Paket Nr. 3	GET heisse-post.com/

Hops

Traceroute
gmx.net

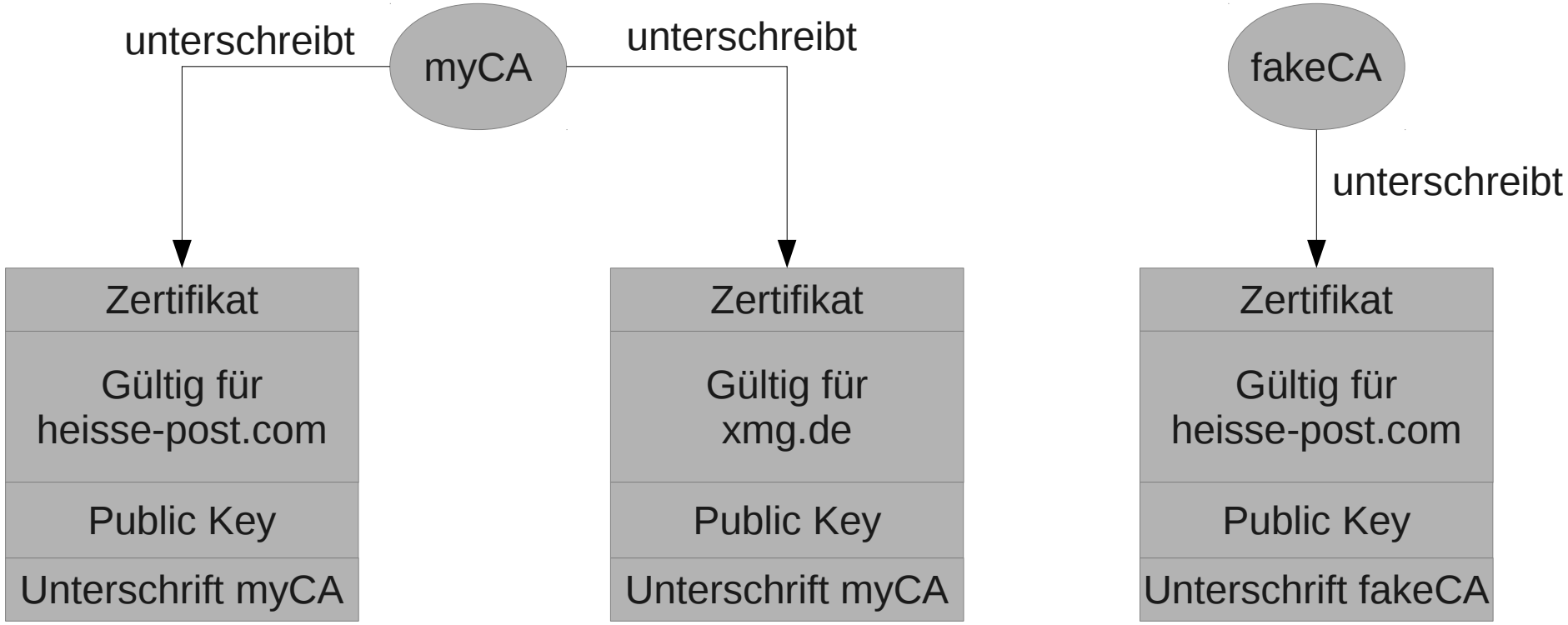


Webzugriffe absichern



Abhören im Internet

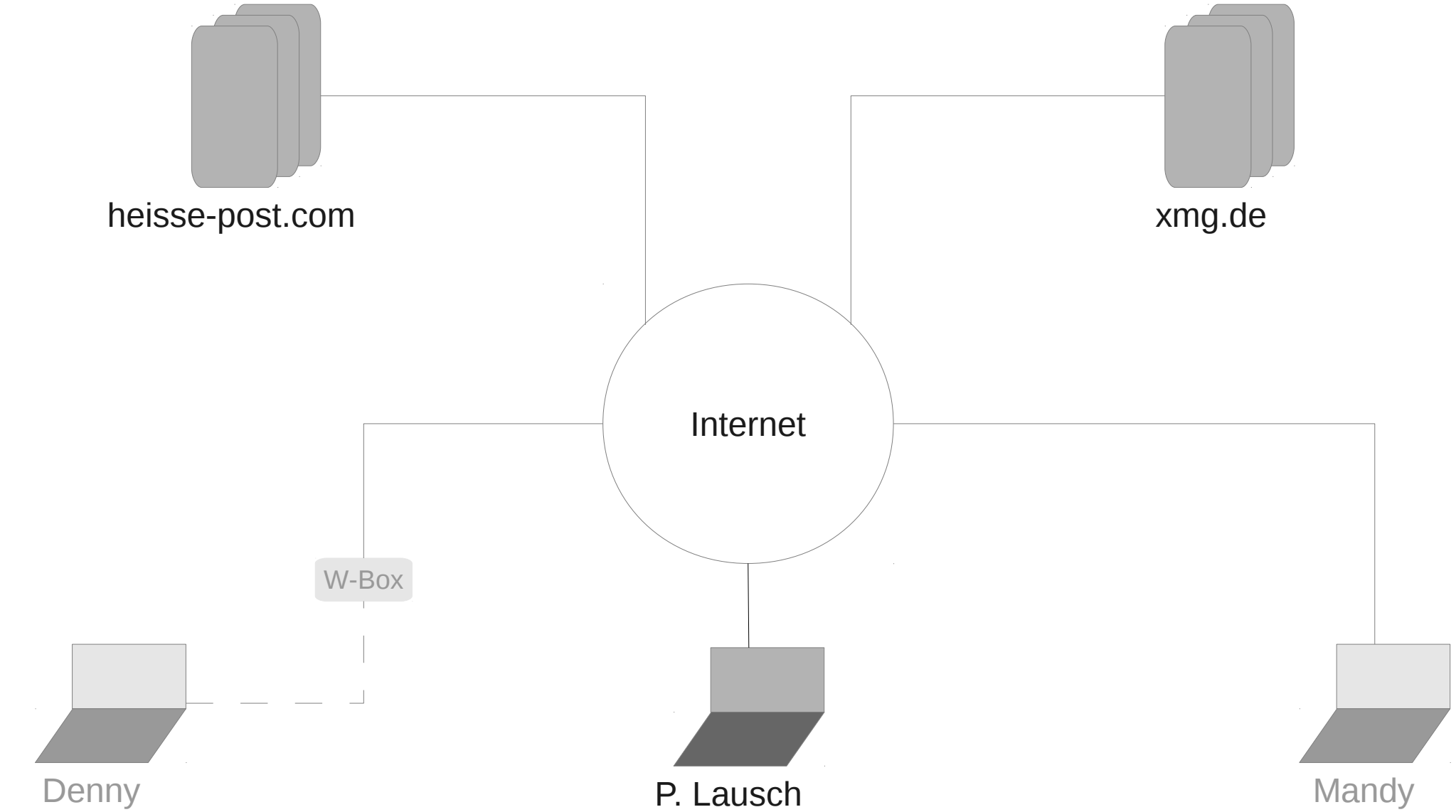
Vorsicht bei Zertifikaten



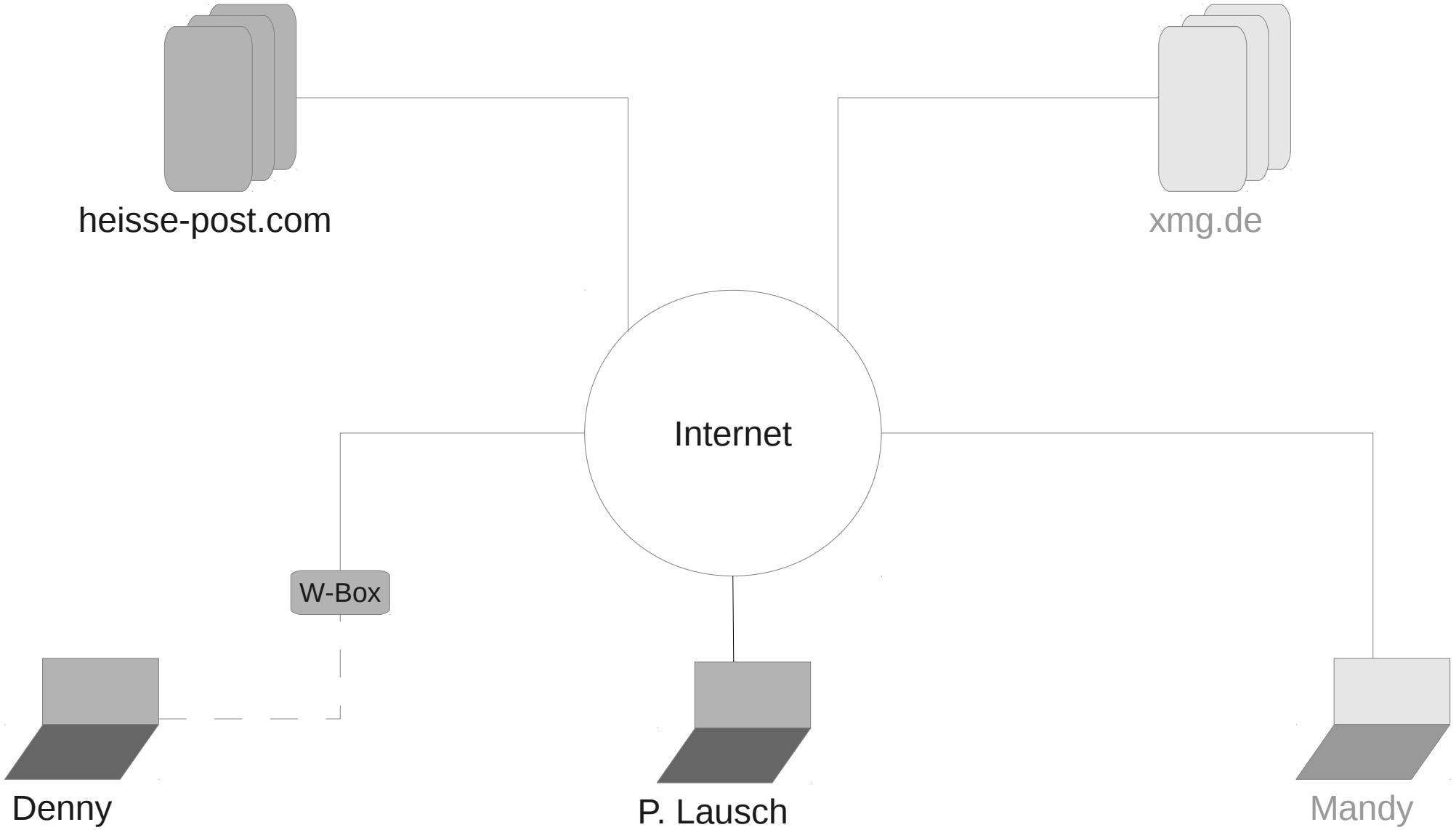
ITU Empfehlung X.509

Schon Fragen?

Providersicherheit

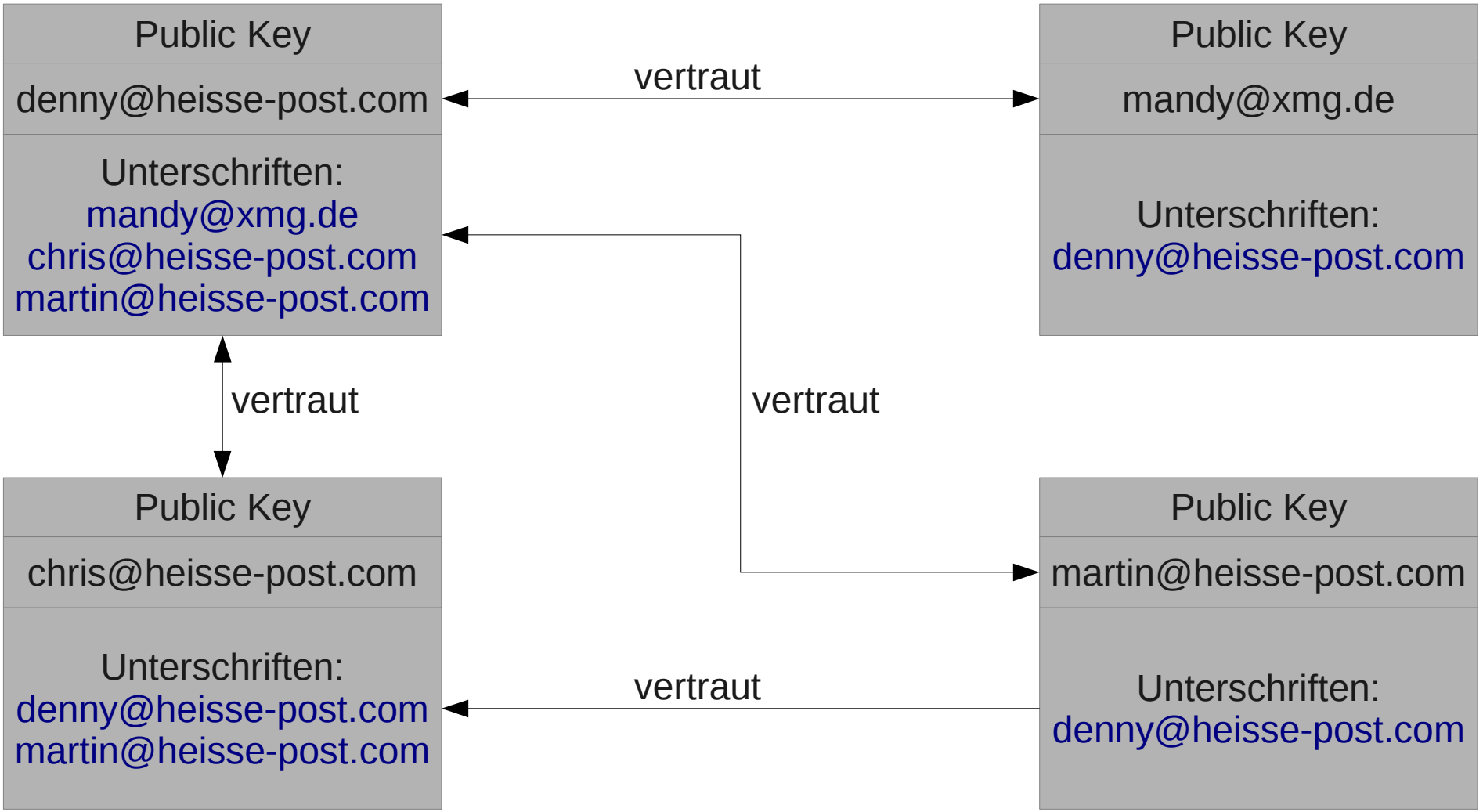


Lokalen Abruf von Mails absichern

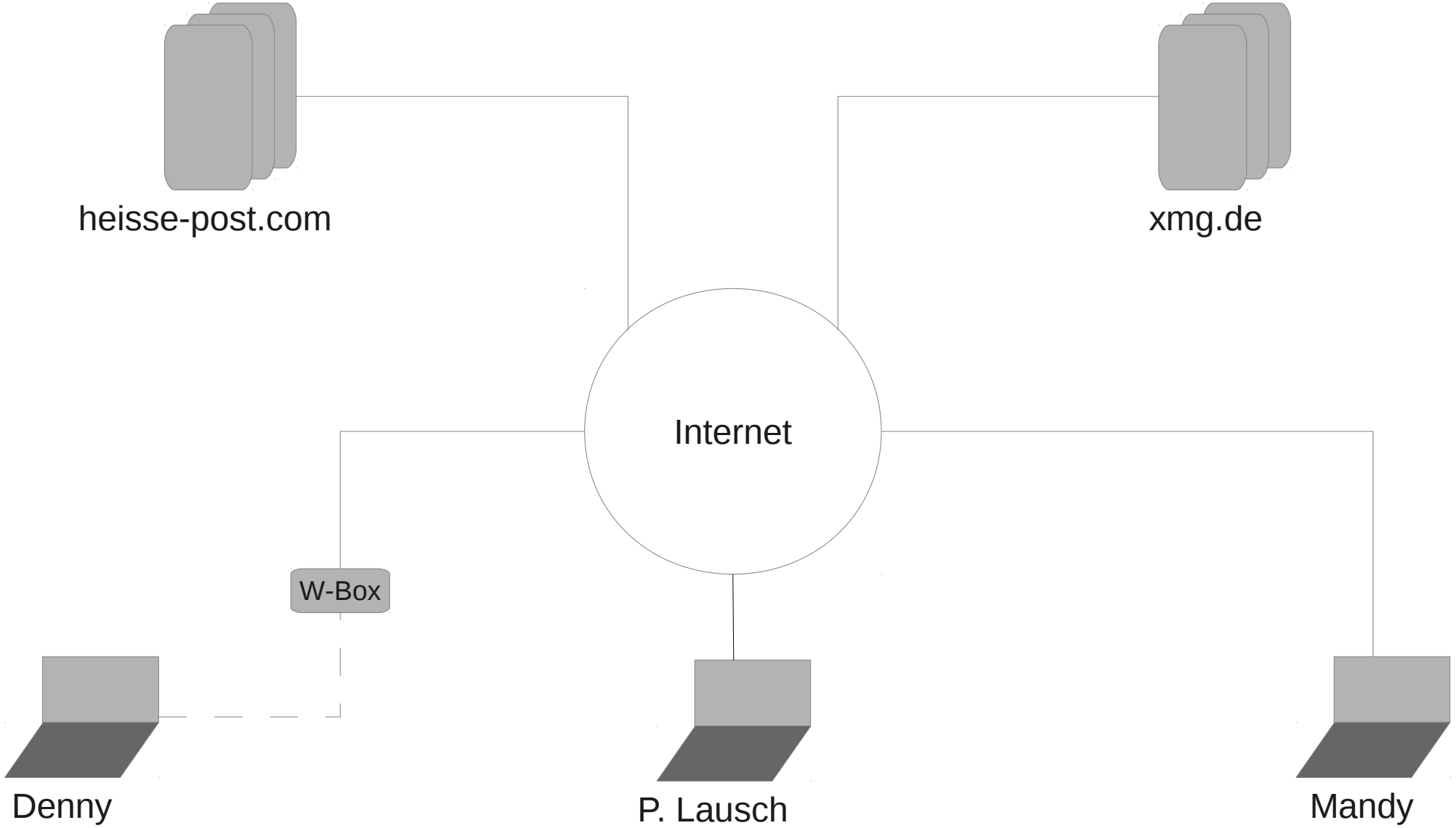


Abhören im Internet

OpenPGP: RFC 4880



Ende-zu-Ende Verschlüsselung



Abhören im Internet

Tools

- Debian Live Builder (http://live.debian.net/)
- Postfix (http://www.postfix.org/)
- Dovecot (http://dovecot.org/)
- Squirrelmail (http://www.squirrelmail.org/)
- Thunderbird (http://www.mozilla.org/thunderbird/)
- GnuPG (http://www.gnupg.org)
- Airodump-ng (http://www.aircrack-ng.org/)
- arpspoof (http://www.monkey.org/~dugsong/dsniff/)
- mitmproxy (http://mitmproxy.org/)
- iptables (https://www.kernel.org/)
- Wireshark (http://www.wireshark.org/)

Noch Fragen?