nic.at

Briefing „Encrypted DNS“

DNS over TLS / DNS over HTTPS

2019-01-15 · Alex Mayrhofer · Head of Research & Development

.at Domain Registry by nic.at · .versicherung by nic.at · RcodeZero DNS by nic.at · TLD Box by nic.at

About nic.at

Domain Registry for „.at“

- Since 1997, ~1.3M Domains

Registry-in-a-Box – new gTLDs

- Operation of .berlin, .hamburg, .versicherung, …

RcodeZero DNS

- Anycast DNS for TLDs and Registrars / ISPs

Research & Community

- Technology, Organisations, Standardization,--

Background

Why DNS encryption was developed

The DNS anno circa 2012

- Sensational Success Story
  - Age 25, and practically unmodified
- Today: „Nothing goes“ without DNS
- Clear text. Everything
  - „DNS is public anyways?“
- 99% UDP, 1% TCP „fallback“
  - Worst TCP support ever!
- DNSSEC? Makes everything secure, doesn‘t it !!?!
  - Does only „sign“, not „encrypt“
- 2013: Snowden revelations
  - NSA: „Clear text PII data … mmmmm…“
  - IETF: „Ohh sheesh – we didn‘t expect *that* scale!“

Photo by Simone Acquaroli on Unsplash

„Pervasive Monitoring is an Attack“

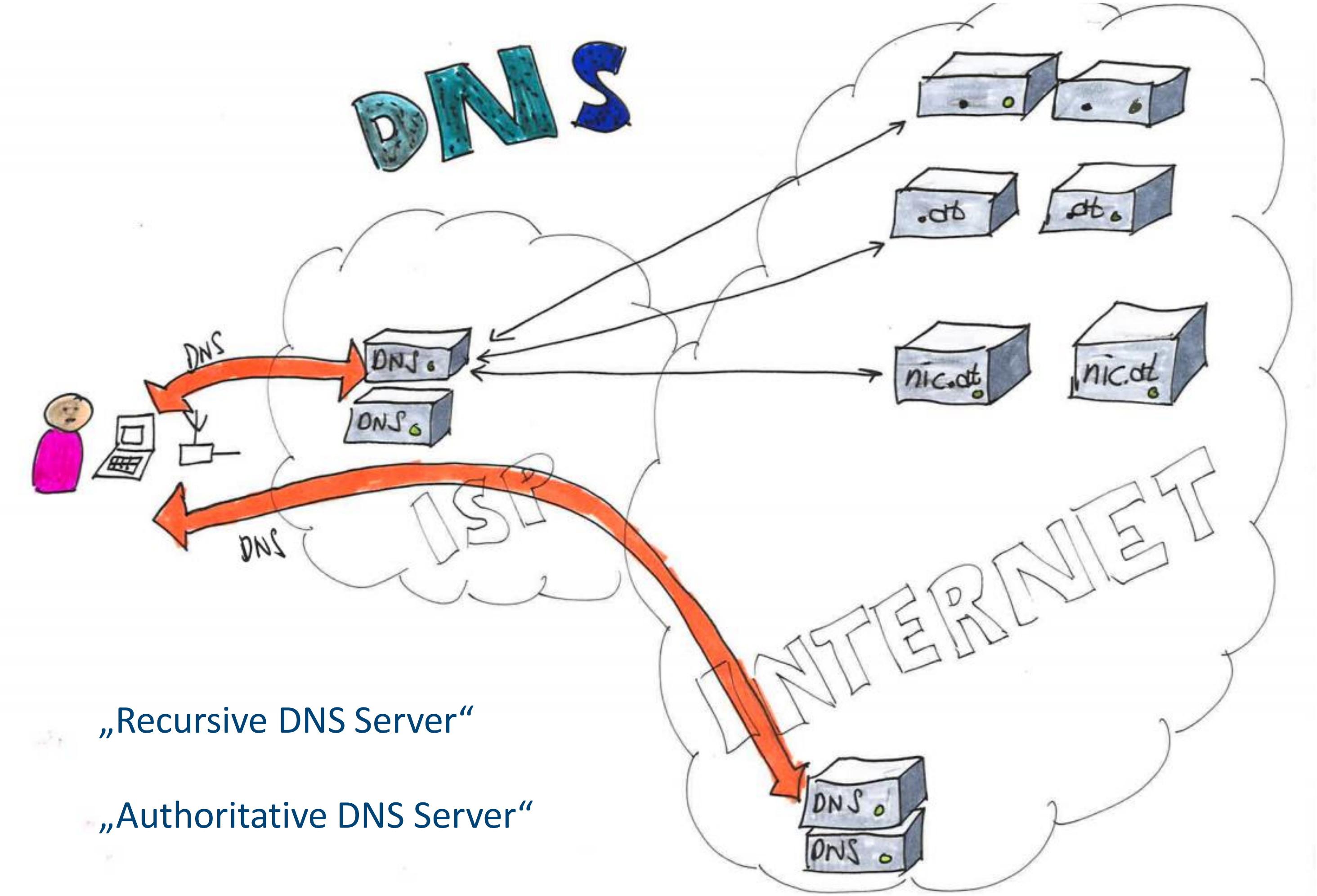
- RFC 7258 – „**Pervasive Monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible**“
- Consequence: Review of all important procotols
- DNS – there‘s not even a standardized *option* for encryption
- Worse – contains „privacy defeating“ mechanism
  - Unneccessarily transmits full QNAME in many cases
  - EDNS(0) Client Subnet
- Leak of Meta-Data & Fingerprinting
  - Re-identification of individuals across networks

Photo by Kote Puerto on Unsplash

„We need encryption“

But where to start?

The DNS Protocol arena

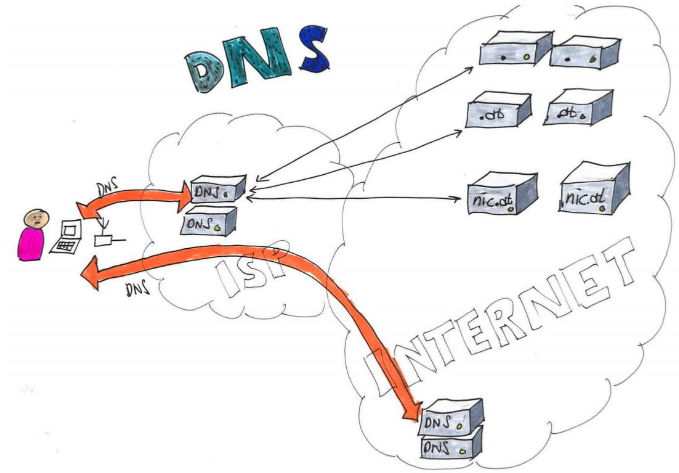


„Recursive DNS Server“

„Authoritative DNS Server“

IETF DPRIVE* („PRIVate Exchange“)

- 2014: „Let‘s deal with the stub resolver to recursor leg“
  - Most significant information leakage
  - 1:few Relation – Authentication simple
  - „Don‘t attempt to boil the ocean“
- 2018: Re-Chartering: Includes „recursive to authoritative“
  - More complex: **m:n** connections (Authentication!)
  - Milestone for end of 2019



*https://datatracker.ietf.org/wg/dprive/about/

DNS over (D)TLS

IETF: DPRIVE / DNSOP / (TLS)

Liste of relevant RFCs

- RFC 7626 – DNS Privacy Considerations (DPRIVE)
- RFC 7766 – TCP Transport for DNS (DNSOP)
- RFC 7816 – QNAME Minimization (DNSOP)
- RFC 7828 – EDNS keepalive (DNSOP)
- RFC 7858 – DNS over TLS (DPRIVE)
- RFC 8094 – DNS over DTLS (DPRIVE)
- RFC 7830 (+RFC 8467) – DNS Padding (DPRIVE)
- RFC 8310 – Usage Profiles
- RFC 8446 – TLS 1.3 (TLS)

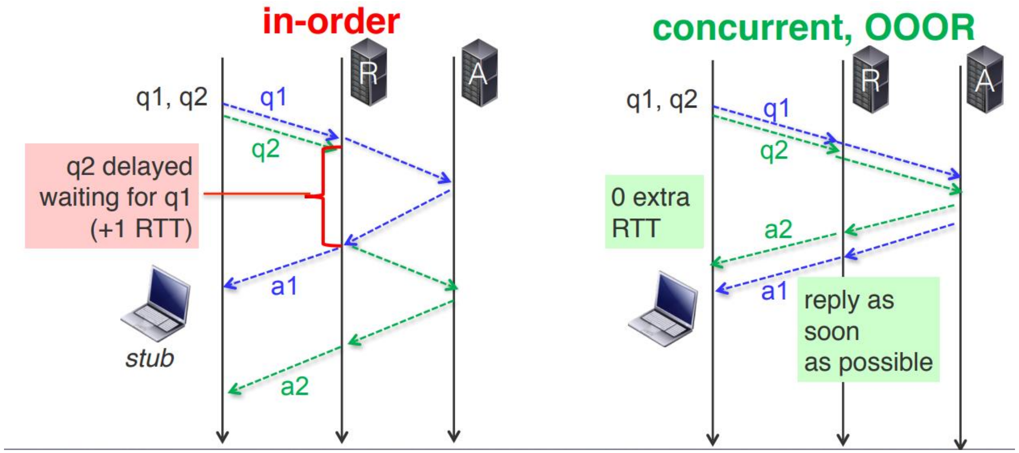
Read this!

RFC 7626 – DNS Privacy Considerations

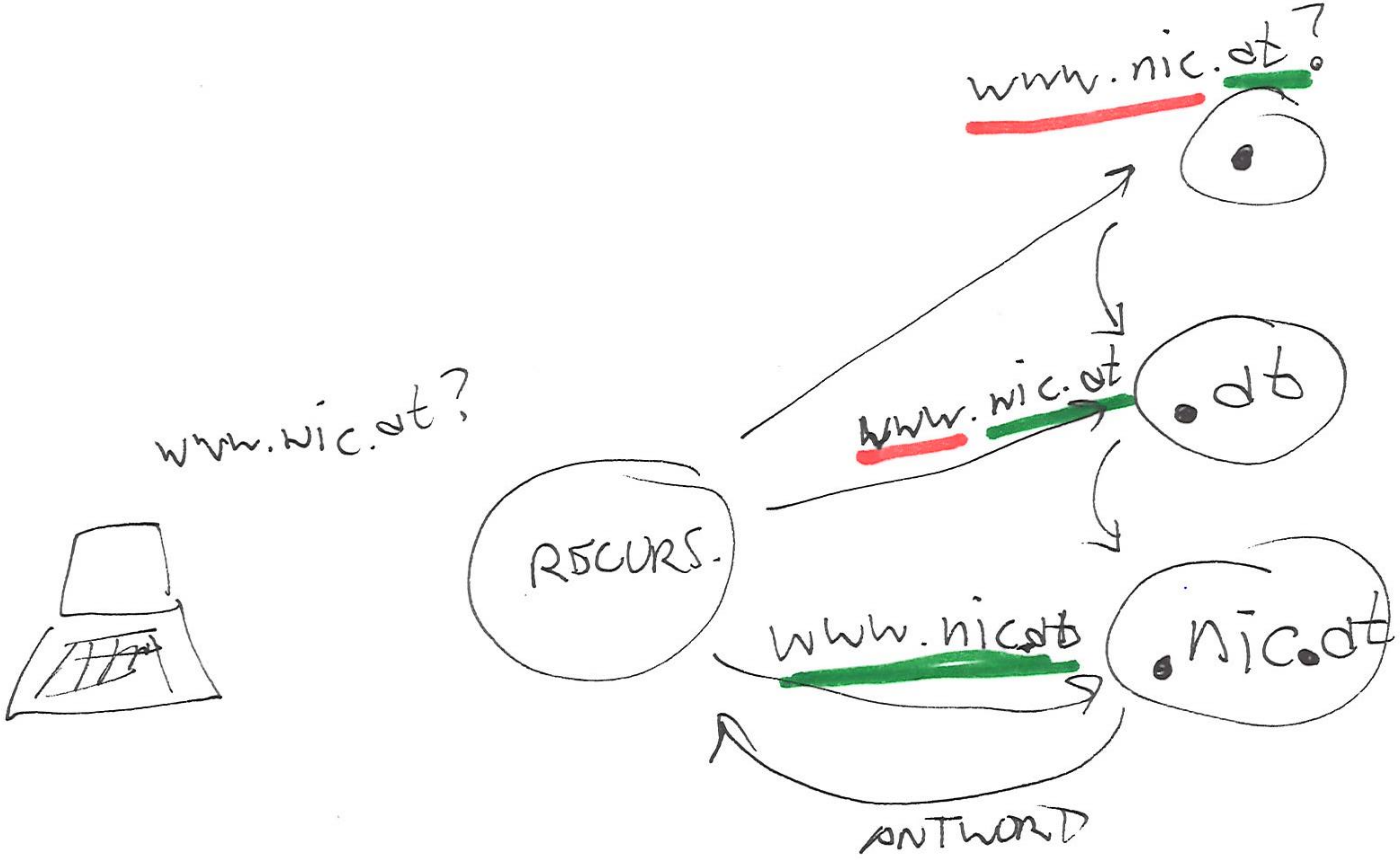
- Privacy aspects / issues in areas of the DNS:
  - In the DNS message (Query Name, IP Adresse)
  - On the server
  - On the Wire
  - Re-Identification based on patterns
- Kills the „DNS is public anyways!“ argument
  - Website of „Alcoholics Anonymous“ is public
  - The fact that someone visits that website regularly is definitely privacy relevant!
- Practical example (similar..)
  - drugstoremorningafterpillvienna16.at
  - (Browser search requests leaking to the DNS?)

RFC 7766 – TCP Transport for DNS

- Goal: Establish DNS over TCP als „first class citizen“
- Features
  - Persistent connections (client soll die schliessen)
  - Connection re-use
  - Pipelining
  - Response Reordering
  - TCP Fast Open
  - Web: „Happy Eyeballs“



RFC 7816 – QNAME Minimization



RFC 7828 – EDNS keepalive

- EDNS Option for Session Management
- For TCP only!
- Clients: „Please leave connection open for X seconds“
- Server: „Ok, leave it open for X seconds“ or „Please close connection now!“

Core spec!

RFC 7858 – DNS over TLS (DoT)

- New Port 853 / TCP
- „On the wire“ protocol is unmodified
- Authentification: Certificates usw? -> RFC 8310
  - „Opportunistic“ vs. „Strict“
  - Chicken/Egg -> Bootstrapping des DoT Servers wie?
- Does not change the „path“ of the DNS message
  - Existing Recursive Nameserver can simply offer an additional, encrypted channel

RFC 8094 – DNS over DTLS

- Port 853 / UDP
- „Same Same but Different“
- Experimental!
  - Issues with fragmentation
  - DTLS is not widely implemented
- Performance advantage of UDP?
  - Mostly because TCP implementation used to be so „lousy“.

DNS over HTTPS

An alternative encryption scheme, driven by browser vendors

Motivation – Browser Vendors

- (a) Browsers do a lot of DNS these days
  - Websites + assets (JS, Ads, Statistics…), CDNs
  - Certificate Validation (OCSP), SafeBrowsing lists, updates, …
  - More direct control over the DNS API desired
- (b) Timing and availability is critical
  - „Happy Eyeballs“ – Slow or lousy (local) DNS servers create bad user experience
  - „Bad Hotel WiFi“ is often „Bad Hotel DNS“…
- (c) DNS is used for censorship
  - Circumventing local (censoring) DNS servers protects Freedom of Speech
  - Eg. Google Jigsaw

IETF DoH* (DNS over HTTPs) group

- Founded 2017
- 2018: RFC 8484
  - – GET or POST
  - – URI Templates (https://dnsserver.example.net/dns-query{?dns})
  - – Wire-Format: application/dns-message (identical zu „normal“ DNS), oder JSON
  - – HTTP Response-Code always 2xx (if successful), no matter which DNS response code

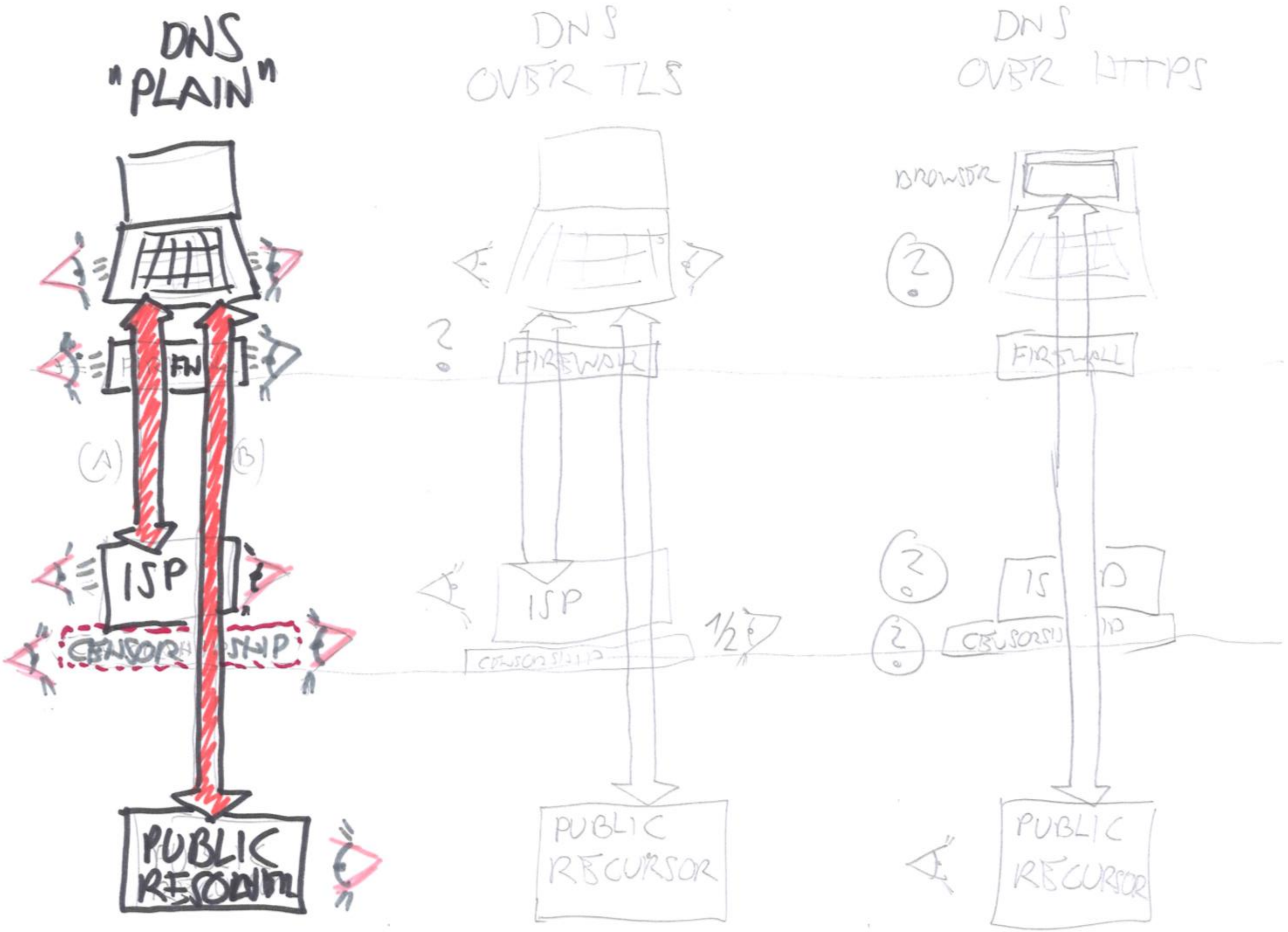
Core spec!

*https://datatracker.ietf.org/wg/doh/about/

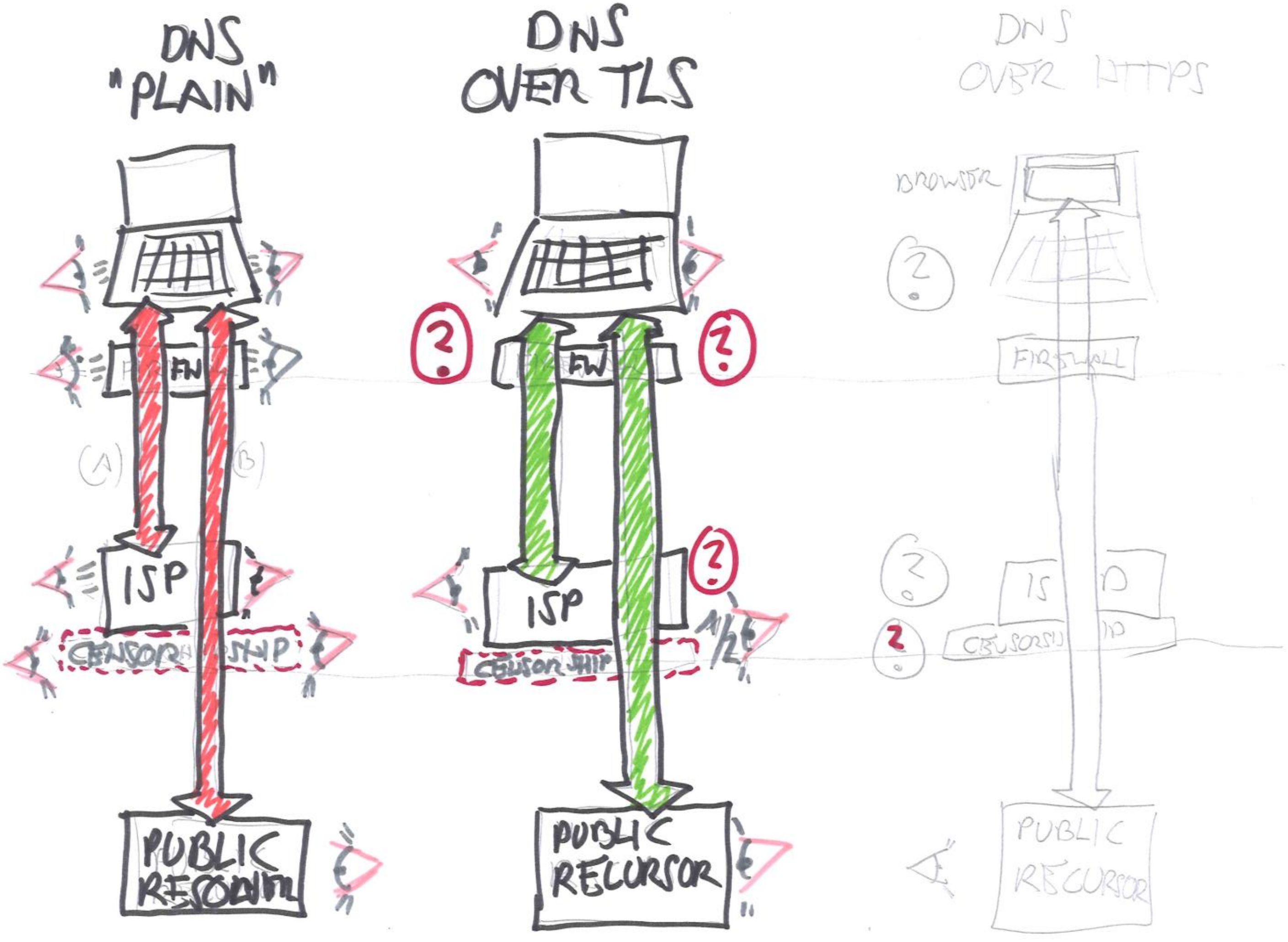
Effects of encrypted DNS

The implications of typical operational models

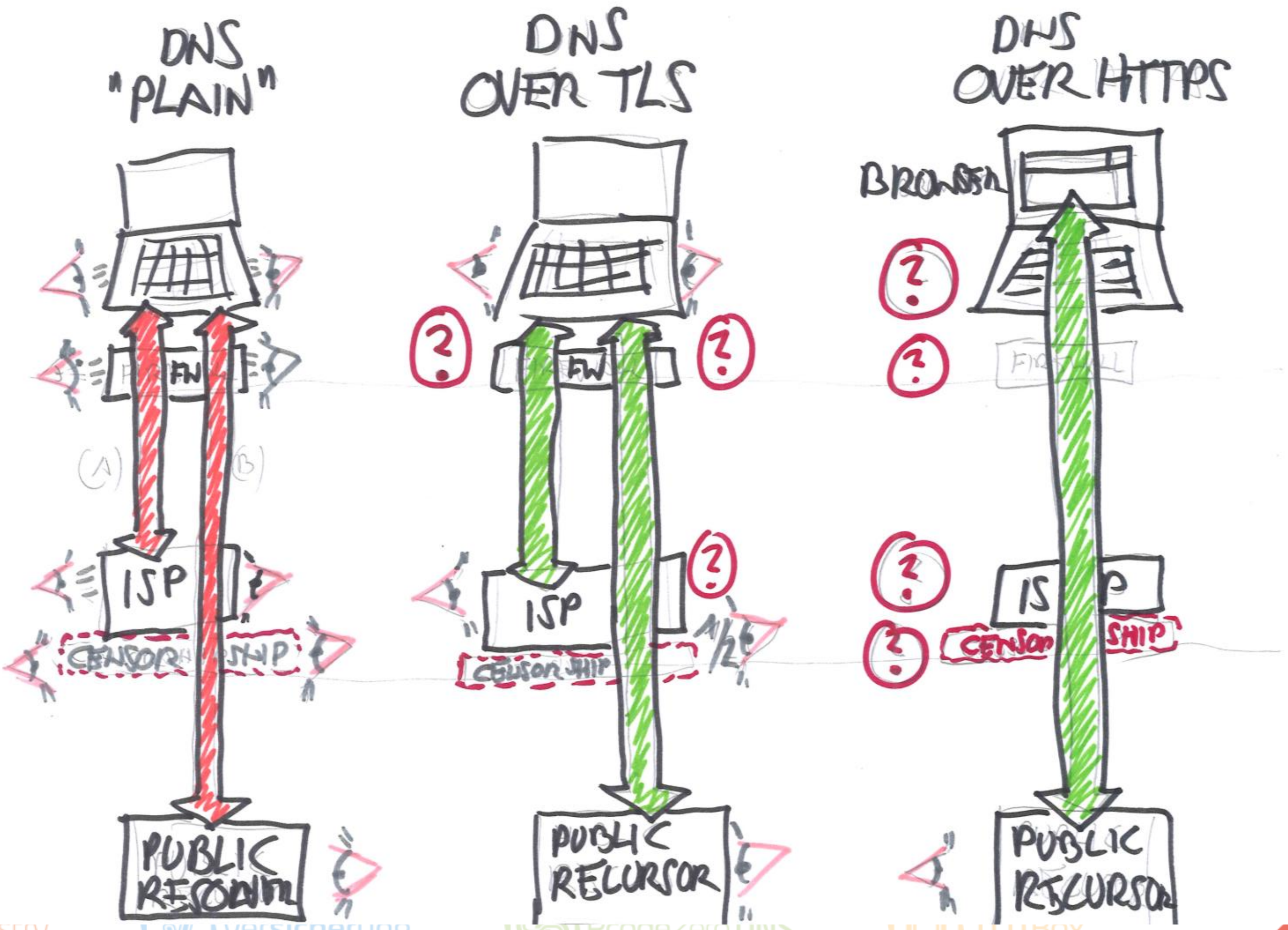
„Plain“ DNS


DNS
"PLAIN"
DNS
OVER TLS
DNS
OVER HTTPS
BROWSER
FW
(A)
(B)
ISP
CENSORSHIP
PUBLIC
RESOLVER
FIREWALL
ISP
CENSORSHIP
1/2
PUBLIC
RECURSOR
FIREWALL
IS P
CENSORSHIP
PUBLIC
RECURSOR

DNS over TLS


DNS "PLAIN"
DNS OVER TLS
DNS OVER HTTPS
BROWSER
FW
FW
FIREWALL
(A)
(B)
?
?
?
?
?
?
ISP
ISP
ISP
CENSORSHIP
CENSORSHIP
CENSORSHIP
1/2
PUBLIC RESOLVER
PUBLIC RECURSOR
PUBLIC RECURSOR

DNS over HTTPS (typical)



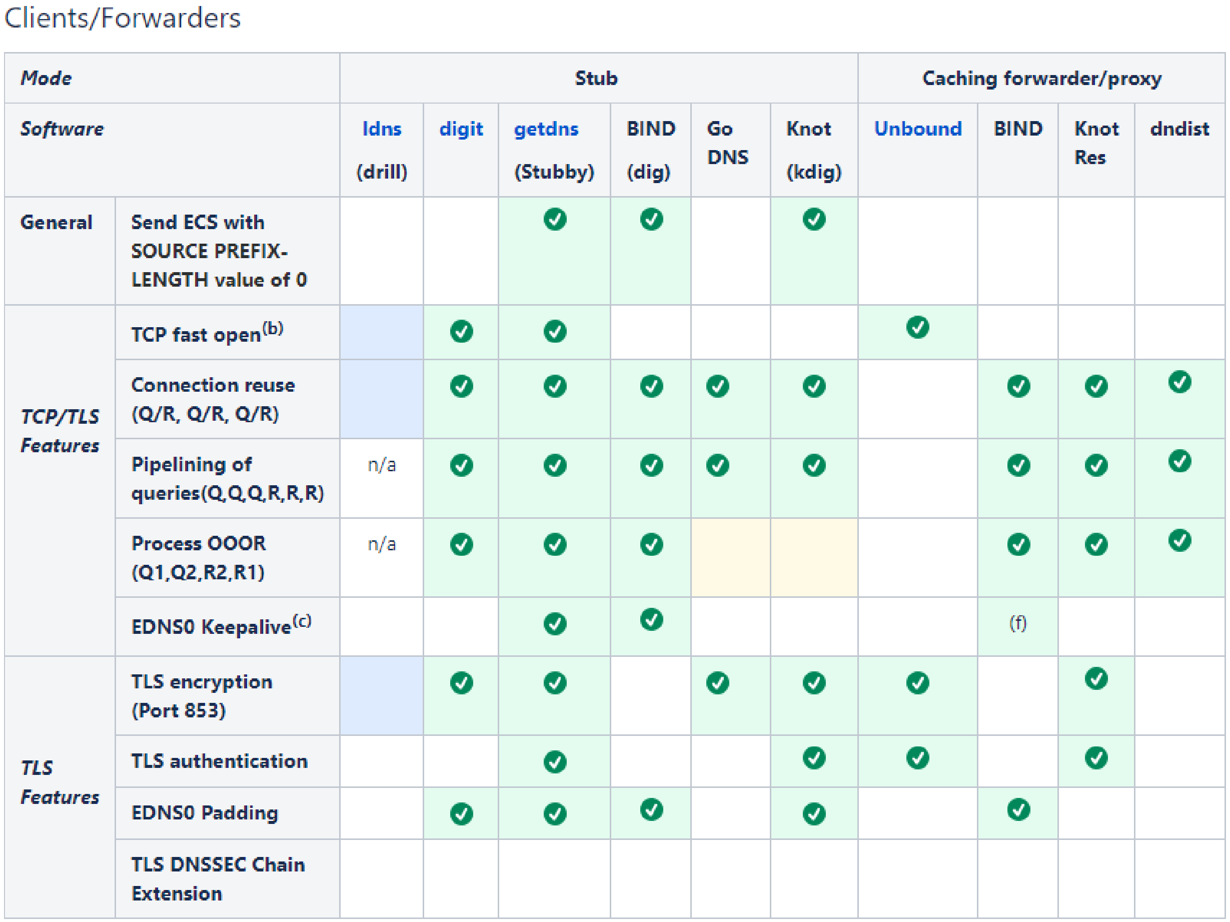
Concerns regarding DoH

- 4 Browser Vendors
- Few big public recursor vendors (1.1.1.1, 8.8.8.8, 9.9.9.9)
- Market concentration / Control?
  - Pre-configured public recursors
  - Example: Mozilla / Cloudflare discussion
- Media echo (German only, sorry!)
  - https://Heise.de/-4203225.html („Die DNS Gruft gehört ausgelüftet“)
  - https://heise.de/-4205380.html („Vom DNS, aktuellen Hypes, Überwachung und Zensur“)

Implementations

Server, Clients, Tools

DoT Clients

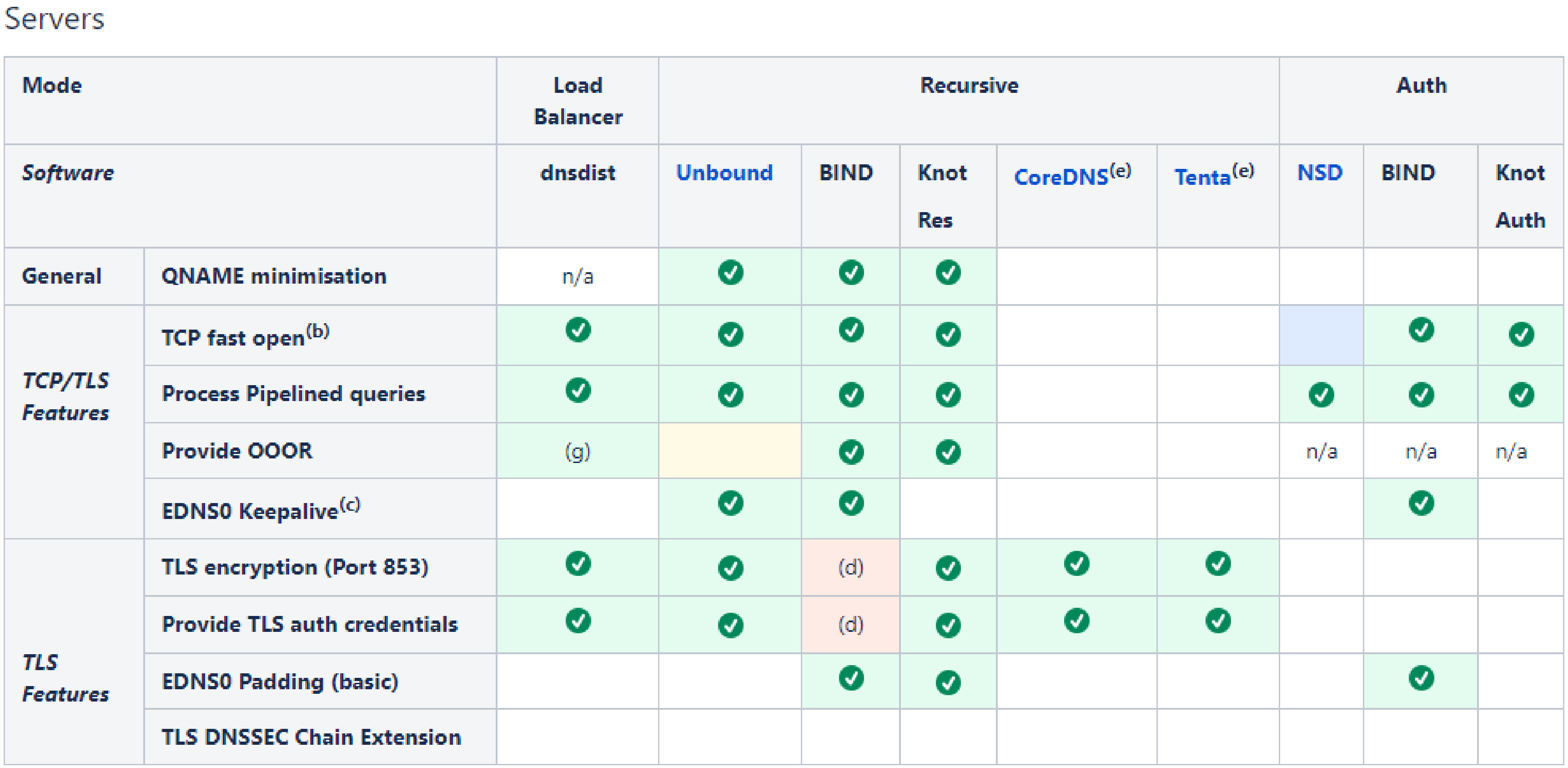


Clients/Forwarders

Mode		Stub						Caching forwarder/proxy			
Software		ldns (drill)	digit	getdns (Stubby)	BIND (dig)	Go DNS	Knot (kdig)	Unbound	BIND	Knot Res	dndist
General	Send ECS with SOURCE PREFIX-LENGTH value of 0			✓	✓		✓				
TCP/TLS Features	TCP fast open(b)		✓	✓				✓			
	Connection reuse (Q/R, Q/R, Q/R)		✓	✓	✓	✓	✓		✓	✓	✓
	Pipelining of queries(Q,Q,Q,R,R,R)	n/a	✓	✓	✓	✓	✓		✓	✓	✓
	Process OOOR (Q1,Q2,R2,R1)	n/a	✓	✓	✓				✓	✓	✓
	EDNS0 Keepalive(c)			✓	✓				(f)		
TLS Features	TLS encryption (Port 853)		✓	✓		✓	✓	✓		✓	
	TLS authentication			✓			✓	✓		✓	
	EDNS0 Padding		✓	✓	✓		✓		✓		
	TLS DNSSEC Chain Extension										

https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Implementation+Status

DoT Server Software



Servers

Mode		Load Balancer	Recursive					Auth		
Software		**dnsdist**	**Unbound**	**BIND**	**Knot Res**	**CoreDNS**[e]	**Tenta**[e]	**NSD**	**BIND**	**Knot Auth**
General	**QNAME minimisation**	n/a	✓	✓	✓					
TCP/TLS Features	**TCP fast open**[b]	✓	✓	✓	✓				✓	✓
	Process Pipelined queries	✓	✓	✓	✓			✓	✓	✓
	Provide OOOR	(g)		✓	✓			n/a	n/a	n/a
	EDNS0 Keepalive[c]		✓	✓					✓	
TLS Features	**TLS encryption (Port 853)**	✓	✓	(d)	✓	✓	✓			
	Provide TLS auth credentials	✓	✓	(d)	✓	✓	✓			
	EDNS0 Padding (basic)			✓	✓				✓	
	TLS DNSSEC Chain Extension									

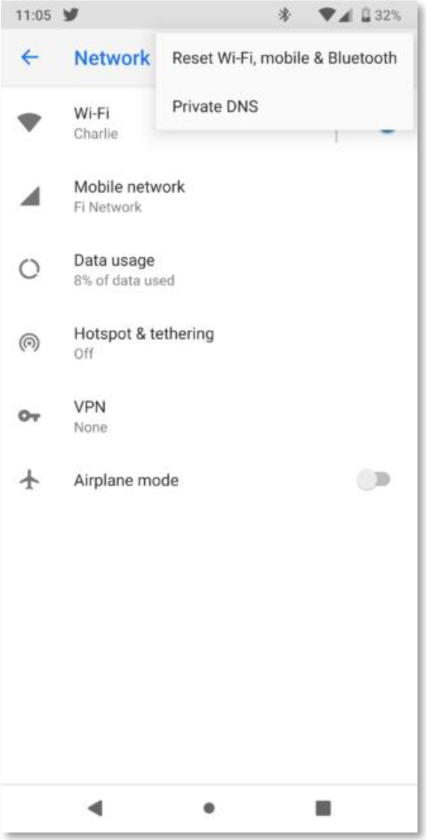
DoT (and DoH) public recursors

- Google DNS (8.8.8.8)
- Cloudflare (1.1.1.1)
- Quad9 (9.9.9.9)
- CleanBrowsing (various, with Filters)

DoH

- Clients
  - Mozilla Firefox
  - Google Chrome
  - (plus test tools)
- Server Software
  - https://github.com/facebookexperimental/doh-proxy
  - https://github.com/curl/curl/wiki/DNS-over-HTTPS#doh-tools

Android 9 – DNS over TLS by default



11:05 32%

Network

Reset Wi-Fi, mobile & Bluetooth

Private DNS

Wi-Fi
Charlie

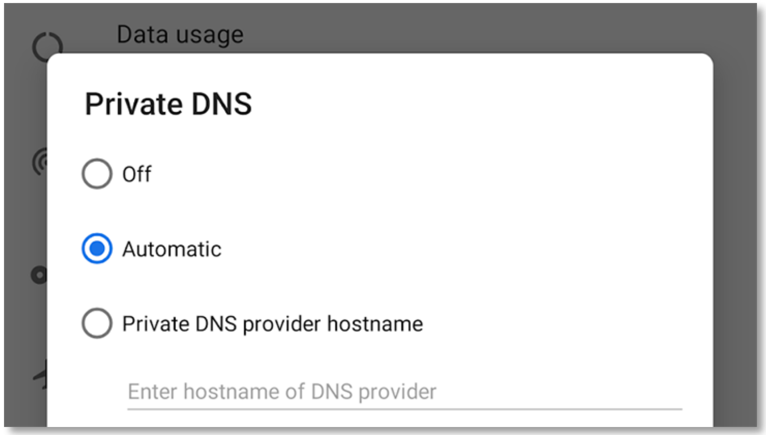
Mobile network
Fi Network

Data usage
8% of data used

Hotspot & tethering
Off

VPN
None

Airplane mode



Data usage

Private DNS

○ Off

● Automatic

○ Private DNS provider hostname

Enter hostname of DNS provider

- Uses DNS over TLS if available on local nameserver
- Falls back to unencrypted DNS if unavailable

Exec Summary

- DNS can now be encrypted, either via TLS or HTTPS
- DNS over HTTPs is more „disruptive“ than DNS over TLS
- Public recursors have implemented either (or both)
  - But few local providers have implemented it (see below :-/)
- Browser Vendors are implementing DNS over HTTPs
  - Ongoing policy discussions around pre-configuration of recursors
- Android 9 implements DNS over TLS *by default*
  - Automatically uses it if available (see above :-/)
  - Google suggesting to configure „dns.google“ manually
- Windows / MacOS – no „out of the box“ solutions – „Stubby“

nic.at

nic.at GmbH

Jakob-Haringer-Str. 8/V · 5020 Salzburg · Austria
T +43 662 4669 -34 · F -29
alexander.mayrhofer@nic.at · **www.nic.at**