

# DNS Privacy Clients

Stubby, Mobile apps and  
beyond!

[dnsprivacy.org](https://dnsprivacy.org)

Sara Dickinson  
Allison Mankin  
Willem Toorop

sara@sinodun.com  
amankin@salesforce.com  
willem@nlnetlabs.com

# Overview

- What do we mean here by DNS Privacy?
- What clients support DNS Privacy today?
  - Comparison of features
  - Shameless plug for Stubby
- Wish list



# DNS Privacy

(stub to recursive)

- Concentrate on **DNS-over-TLS** ([RFC7858](#))
  - No implementations of DNS-over-DTLS ([RFC8094](#))
  - DNSCrypt not standard, HTTPS, QUIC
- **Good TCP** ([RFC7766](#), [RFC7828](#))
  - Pipeline queries over ‘persistent connections’, handle OOR, TCP Fast open, etc.
- **Good TLS** ([RFC7525](#), TLS 1.2, Session resumption)

# DNS Privacy

(stub to recursive)

- **EDNS0 Padding** to hide msg size ([RFC7830](#), [draft](#))
- **EDNS0 Client Subnet** (to prevent ECS upstream)
- **TLS authentication** of server ([draft-tls-profiles](#))
  - Authentication name/SPKI pinset  
DANE, [TLS DNSSEC Chain Extension](#)
  - Strict vs Opportunistic Usage profile


# Authentication in DNS-over-TLS

Profiles draft defines 2 Usage profiles:

- Strict
  - “Do or do not. There is no try.”
- Opportunistic
  - “Success is stumbling from failure to failure with no loss of enthusiasm”

# Authentication in DNS-over-TLS

Profiles draft defines 2 Usage profiles:

- Strict  (Encrypt & Authenticate) or Nothing
  - “Do or do not. There is no try.”
- Opportunistic
  - “Success is stumbling from failure to failure with no loss of enthusiasm”

# Authentication in DNS-over-TLS

Profiles draft defines 2 Usage profiles:

- Strict  (Encrypt & Authenticate) or Nothing
  - “Do or do not. There is no try.”
- Opportunistic  Try in order:
  1. Encrypt & Authenticate then
  2. Encrypt then
  3. Clear text
  - “Success is stumbling from failure to failure with no loss of enthusiasm”

# DNS Privacy Client Usability

- DNS Privacy is a new paradigm for end users
- End users are a new paradigm for DNS people!



# DNS Privacy Client Usability

- DNS Privacy is a new paradigm for end users
  - End users are a new paradigm for DNS people!
- 
- Uptake critically dependant on clients being usable
  - **'Usable Security'**: Good GUIs aren't enough - users still struggle with the basics if they don't understand what they are doing (DNSSEC, HTTPS, PGP)

# Flavours of client

- Desktop system resolvers
- Command line tools/libraries/forwarders
- Mobile

**DISCLAIMER!!** Not exhaustive, other DNS clients are available.....  
All data here are to the best of my knowledge! Please send  
corrections/updates/additions to [sara@sinodun.com](mailto:sara@sinodun.com)



# Desktop System resolvers

	TLS support
Linux	✗ libc, systemd*
macOS	✗
Windows	✗



# Desktop System resolvers

	TLS support
Linux	✗ libc, systemd*
macOS	✗
Windows	✗

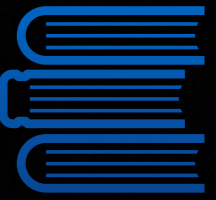
But then again, think about DNSSEC support.....



# Command line tools

Features					
		getdns_query	kdig	delv (dig)	drill
DNS	ECS privacy	Dark Green	Dark Green	9.12	Grey
TCP	Pipelining	Dark Green	Dark Green	Dark Green	Light Green
	OOOR	Dark Green	Dark Green	Dark Green	Grey
	Keepalive/DSO	Dark Green	Grey	9.12	Grey
	TCP Fast Open	Dark Green	Dark Green	9.12	Grey
TLS	TLS	Dark Green	Dark Green	Grey	Light Green
	Authentication	Dark Green	Dark Green	Grey	Grey
	Strict vs Oppo	Dark Green	Grey	Grey	Grey
	EDNS0 Padding	Dark Green	Dark Green	9.12	Grey

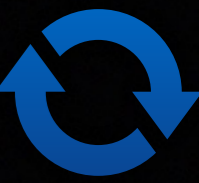
- Dark Green: Latest stable release supports this
- Light Green: Patch available
- Yellow: Patch/work in progress
- Grey: Not applicable or not yet planned



# Libraries

Features						
		getdns	libknot	libunbound	ldns	dnsmasq
DNS	ECS Privacy	Dark Green	Dark Green	Grey	Grey	Grey
	Pipelining	Dark Green	Dark Green	Grey	Light Green	Grey
TCP	OOOR	Dark Green	Dark Green	Grey	Grey	Grey
	Keepalive/DSO	Dark Green	Grey	Grey	Grey	Grey
	TCP Fast Open	Dark Green	Dark Green	Dark Green	Grey	Grey
TLS	TLS	Dark Green	Dark Green	Dark Green	Light Green	Grey
	Authentication	Dark Green	Dark Green	Grey	Grey	Grey
	Strict vs Oppo	Dark Green	Grey	Grey	Grey	Grey
	EDNS0 Padding	Dark Green	Dark Green	Dark Green	Grey	Grey

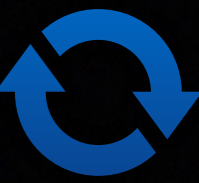
- Dark Green: Latest stable release supports this
- Light Green: Patch available
- Yellow: Patch/work in progress
- Grey: Not applicable or not yet planned



# Local forwarders

Features		Stub		
		stubby (getdns)	unbound	proxy (stunnel)
DNS	ECS Privacy	Dark Green	Grey	Grey
	Pipelining	Dark Green	Grey	Dark Green
TCP	OOOR	Dark Green	Grey	Dark Green
	Keepalive/DSO	Dark Green	Grey	Grey
	TCP Fast Open	Dark Green	Dark Green	Grey
TLS	TLS	Dark Green	Dark Green	Dark Green
	Authentication	Dark Green	Grey	Dark Green
	Strict vs Oppo	Dark Green	Grey	Grey
	EDNS0 Padding	Dark Green	Dark Green	Grey

- Dark Green: Latest stable release supports this
- Light Green: Patch available
- Yellow: Patch/work in progress
- Grey: Not applicable or not yet planned



# Local forwarders

Features		Stub		
		stubby (getdns)	unbound	proxy (stunnel)
DNS	ECS Privacy	Dark Green	Grey	Grey
	Pipelining	Dark Green	Grey	Dark Green
TCP	OOOR	Dark Green	Grey	Dark Green
	Keepalive/DSO	Dark Green	Grey	Grey
	TCP Fast Open	Dark Green	Dark Green	Grey
TLS	TLS	Dark Green	Dark Green	Dark Green
	Authentication	Dark Green	Grey	Dark Green
	Strict vs Oppo	Dark Green	Grey	Grey
	EDNS0 Padding	Dark Green	Dark Green	Grey

- Dark Green: Latest stable release supports this
- Light Green: Patch available
- Yellow: Patch/work in progress
- Grey: Not applicable or not yet planned

Knot resolver support  
coming soon!





# Mobile

	Native support	Apps
Android	IETF 99 Hackathon: WIP on Opportunistic DNS-over-TLS	
iOS		Work inProgress!! Wrapper around Stubby: <a href="https://dnssdisco.com">dnssdisco.com</a> , <a href="#">GitHub repo</a>



# Stubby



- A privacy enabling stub resolver: [User Guide](#)
- From [getdns](#) team, but is now a [standalone application](#)
  - And a movie ([Stg. Stubby movie](#))
- Daemon listening on localhost, TLS proxy
- Comes with config for [experimental servers](#), including authentication information (Strict is easy)

# Stubby status



- **Command line** tool - for 'advanced' users
  - 1.2 release: Stability improvements, YAML for config
- **Linux** Packages for getdns, not yet for Stubby
- **macOS**: [Homebrew formula](#) for stubby service **NEW!**
- **Windows binary** **NEW!**
- **macOS**: [GUI prototype](#) **NEW!**

# Stubby status



- **Command line** tool - for 'advanced' users
  - 1.2 release: Stability improvements, YAML for config
- **Linux** Packages for getdns, not yet for Stubby
- **macOS**: [Homebrew formula](#) for stubby service **NEW!**
- **Windows binary** **NEW!**
- **macOS**: [GUI prototype](#) **NEW!**

**Funded by NLnet  
Foundation and Salesforce!**

# Subby GUI preview

Prototype!  
HELP WANTED

StubbyManager

Service Status: **Running**    Start    Stop


Test    Restart

---

DNS Servers:     Use Stubby DNS

Start the service then check this box and Apply settings to start using Stubby DNS.

Hit the Stop button to return to default DNS settings.



Advanced...    View the log...

---

Revert to default    Revert    Apply

```
# Ordered list composed of one or more transport protocols.
dns_transport_list:
- GETDNS_TRANSPORT_TLS

# Selects Strict or Opportunistic Usage profile.
tls_authentication: GETDNS_AUTHENTICATION_REQUIRED

# EDNS0 option to pad the size of the DNS query.
tls_query_padding_blocksize: 256

# EDNS0 option for ECS client privacy.
edns_client_subnet_private : 1

# EDNS0 option for keepalive idle timeout in ms.
idle_timeout: 10000

# Set the listen addresses for the stubby DAEMON.
listen_addresses:
- 127.0.0.1
- 0::1

# Instructs stubby to distribute queries across all available name servers.
round robin upstreams: 1
```

Validate Config    Cancel    OK

Stubby Log

```
[12:36:02.363204] STUBBY: 145.100.185.15 : Upstream : TLS - Resps= 1, Timeouts = 0, Best_auth =Success
[12:36:02.363218] STUBBY: 145.100.185.15 : Upstream : TLS - Conns= 1, Conn_fails= 0, Conn_shuts= 0, Backoffs = 0
[12:36:06.218999] STUBBY: 145.100.185.16 : Conn opened: TLS - Strict Profile
[12:36:16.373990] STUBBY: 145.100.185.16 : Conn closed: TLS - Resps= 1, Timeouts = 0, Curr_auth =Success, Keepalive(ms)= 10000
[12:36:16.374026] STUBBY: 145.100.185.16 : Upstream : TLS - Resps= 1, Timeouts = 0, Best_auth =Success
[12:36:16.374031] STUBBY: 145.100.185.16 : Upstream : TLS - Conns= 1, Conn_fails= 0, Conn_shuts= 0, Backoffs = 0
[12:36:18.410175] STUBBY: 185.49.141.37 : Conn opened: TLS - Strict Profile
[12:36:28.657808] STUBBY: 185.49.141.37 : Conn closed: TLS - Resps= 1, Timeouts = 0, Curr_auth =Success, Keepalive(ms)= 10000
[12:36:28.657852] STUBBY: 185.49.141.37 : Upstream : TLS - Resps= 1, Timeouts = 0, Best_auth =Success
[12:36:28.657857] STUBBY: 185.49.141.37 : Upstream : TLS - Conns= 1, Conn_fails= 0, Conn_shuts= 0, Backoffs = 0
```

# Test DNS Privacy servers

## Project dnsprivacy-monitoring

\* Green indicates success

\* Red indicates failed test (this might result from non DNS related issues such server being off line, blocking from the probe location, etc.) Note that the 'Strict mode' tests could fail for a number of reasons including incorrect credentials, self-signed certificates for name only authentication, incompatible TLS version or Cipher suites, etc. The console log of the test may give more information.

\* Grey indicates test not run (e.g. due to lack of available transport or the lack of the SPKI pin)

Authentication information is taken from <https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Test+Servers>

These tests use Stephane Bortzmeyer's nagios plugin - see <https://github.com/bortzmeyer/monitor-dns-over-tls>

Configuration Matrix		Responds over TLS	Strict mode - Name only	Strict mode - SPKI only	Certificate expiry > 0 days	Certificate expiry > 14 days	QNAME minimisation used
getdnsapi.net	v6	✓	✓	✓	✓	✓	✓
	v4	✓	✓	✓	✓	✓	✓
dnsovertls.sinodun.com	v6	✓	✓	✓	✓	✓	!
	v4	✓	✓	✓	✓	✓	!
dnsovertls1.sinodun.com	v6	✓	✓	✓	✓	✓	!
	v4	✓	✓	✓	✓	✓	!
dns.cmrg.net	v6	✓	✓	✓	✓	✓	✓
	v4	✓	✓	✓	✓	✓	!
tls-dns-u.odvr.dns-oarc.net	v6	✓	!	!	✓	✓	!
	v4	✓	!	!	✓	✓	!
dns-resolver.yeti.eu.org	v6	✓	✓	✓	✓	✓	✓
	v4	⊘	⊘	⊘	⊘	⊘	⊘
yeti-rr.datev.net	v6	✓	✓	✓	✓	✓	✓
	v4	⊘	⊘	⊘	⊘	⊘	⊘
unicast.censurfridns.dk	v6	✓	✓	⊘	✓	✓	!
	v4	✓	✓	⊘	✓	✓	!
dns-tls.openbsd.se	v6	⊘	⊘	⊘	⊘	⊘	⊘
	v4	✓	✓	✓	✓	✓	!



Details on  
[dnsprivacy.org](https://dnsprivacy.org):  
[DNS Test Servers](#)

# Wish list

- Windows support (targeting non-technical users)
- iOS: Native support
- ‘Large open resolver’ offering DNS-over-TLS
- Usable security research on DNS Privacy ([NDSS 2018](#))
- More testing at IETF 100!!

# Thank you!

Any Questions?

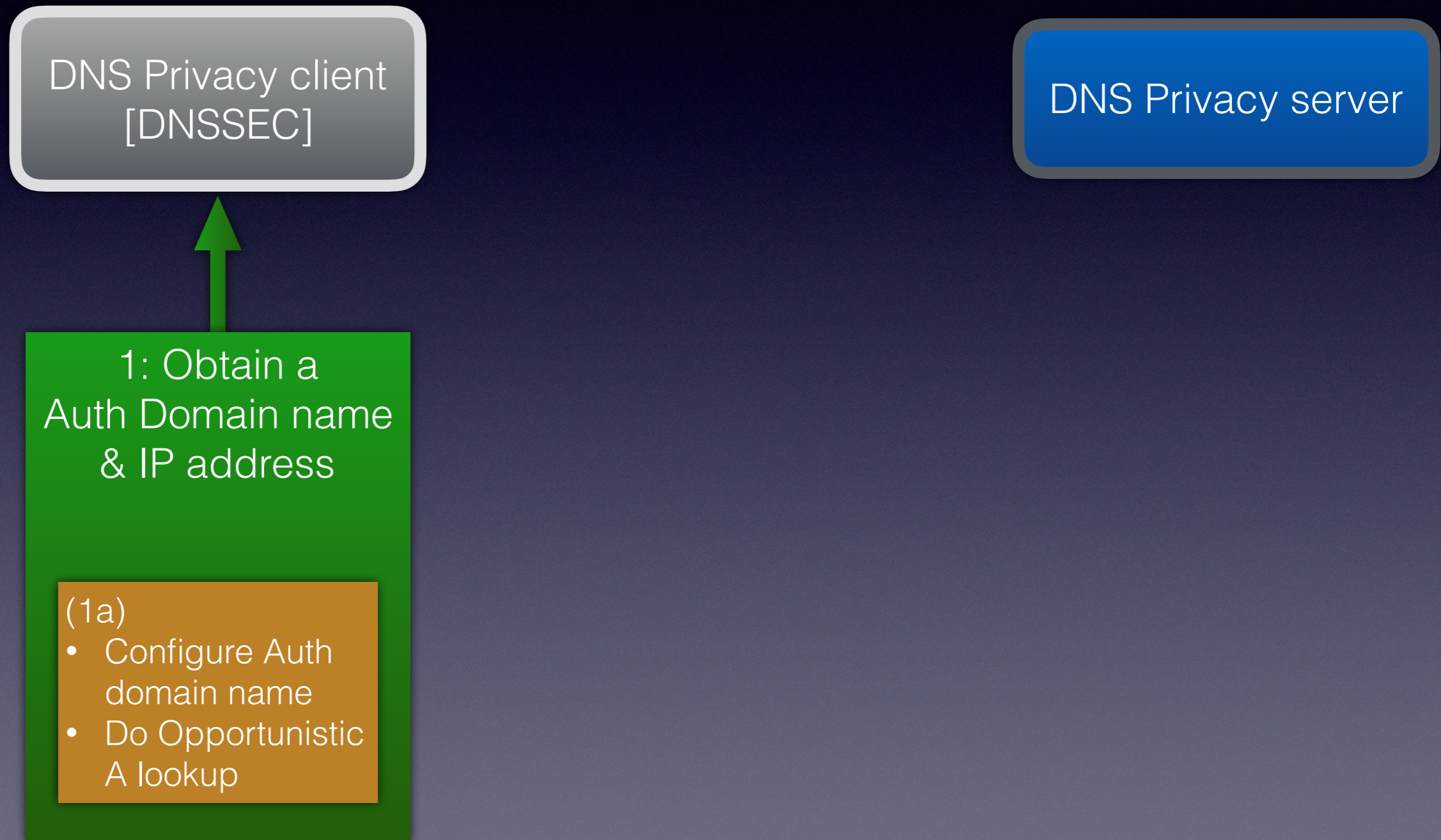
[dnspriivacy.org](https://dnspriivacy.org)



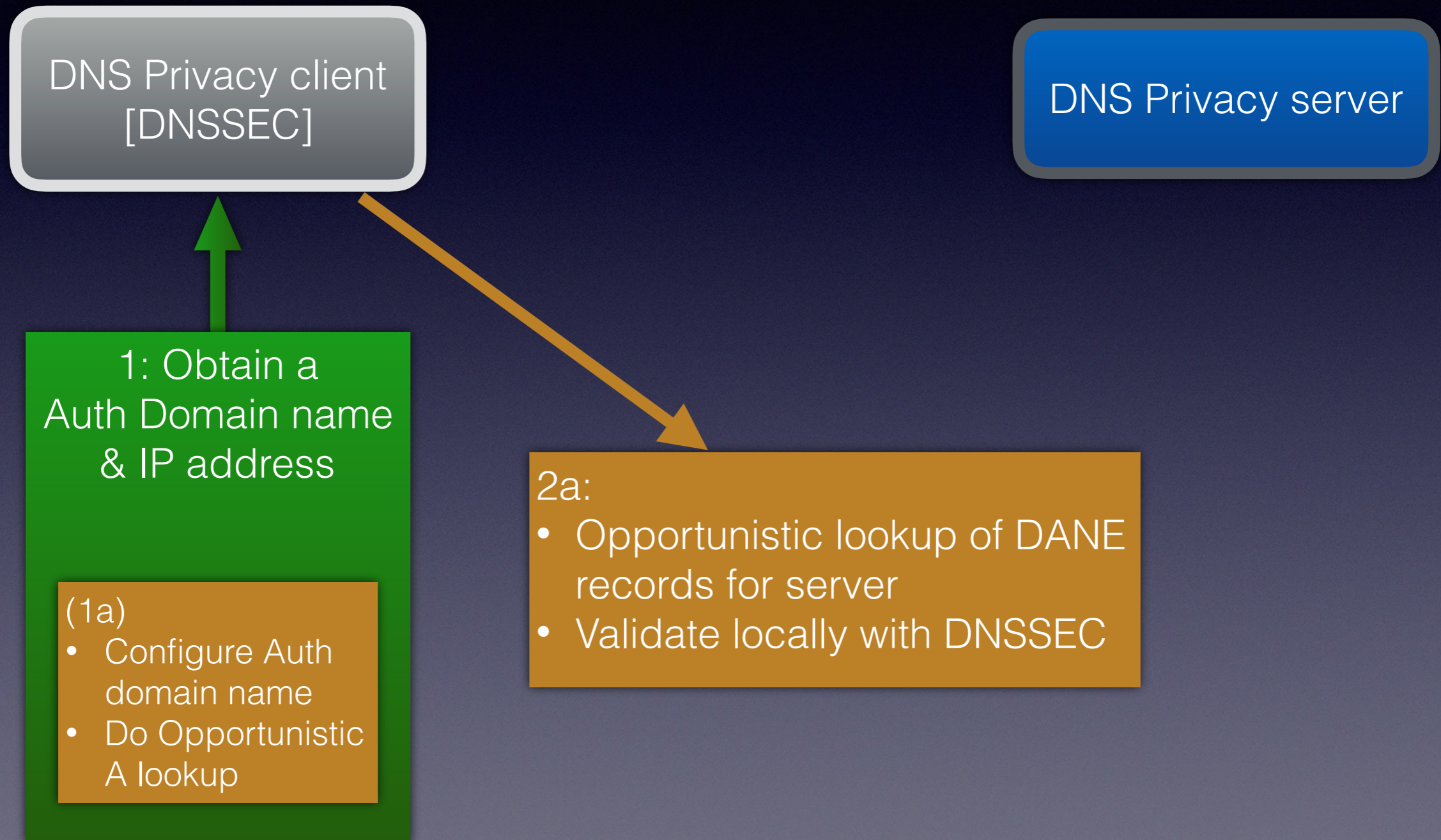


Additional slides

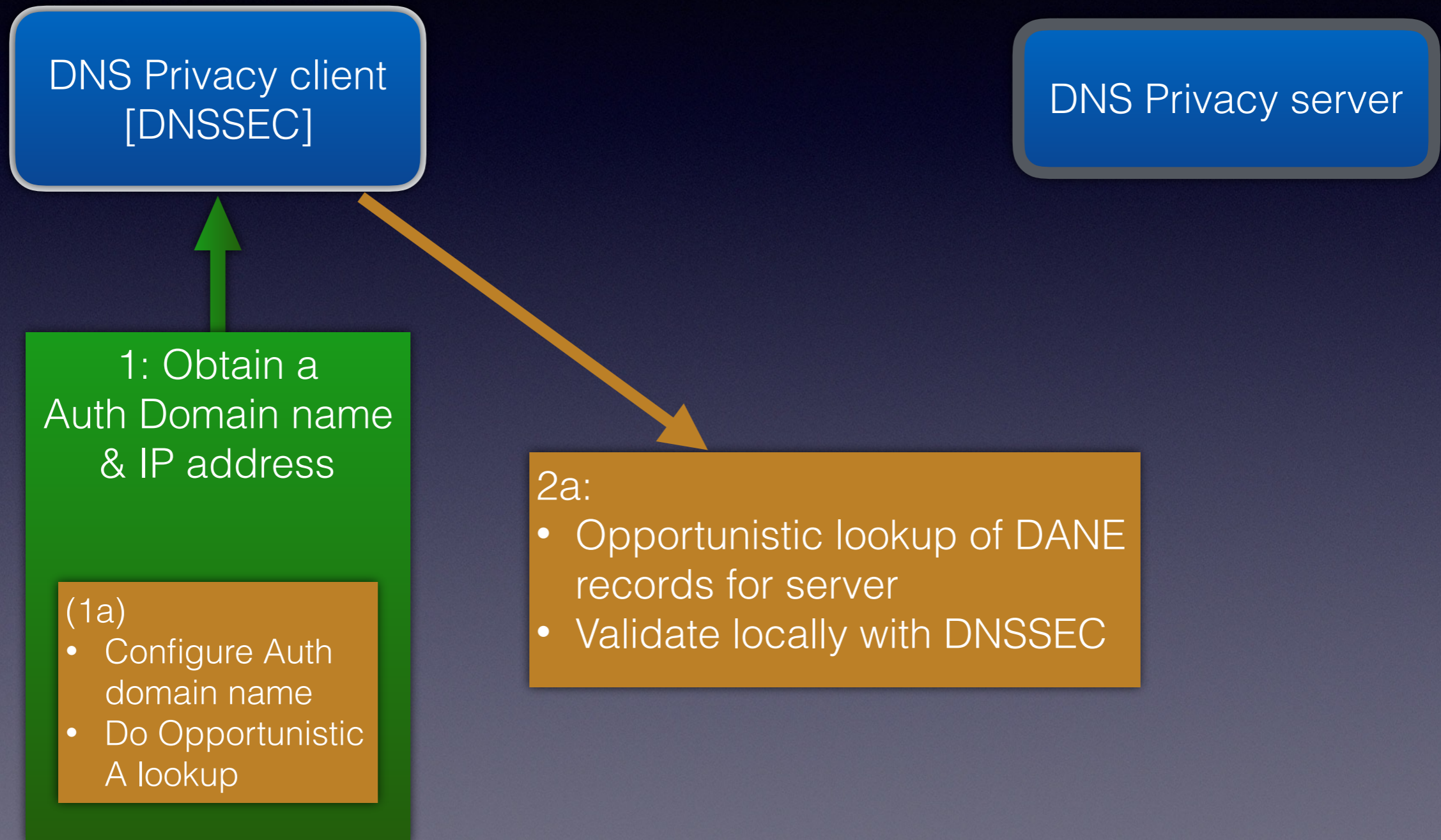
# DNS Auth using DANE



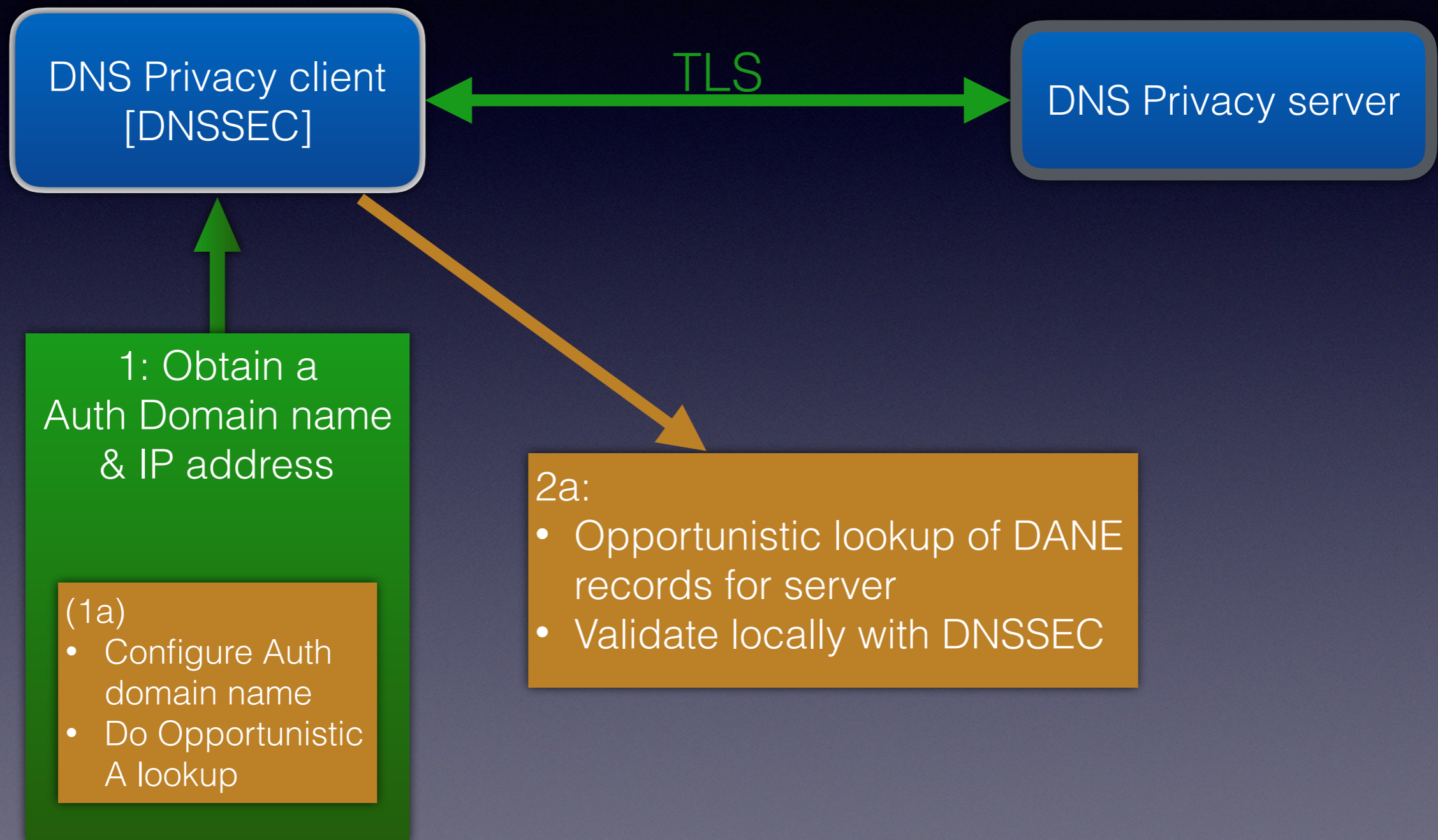
# DNS Auth using DANE



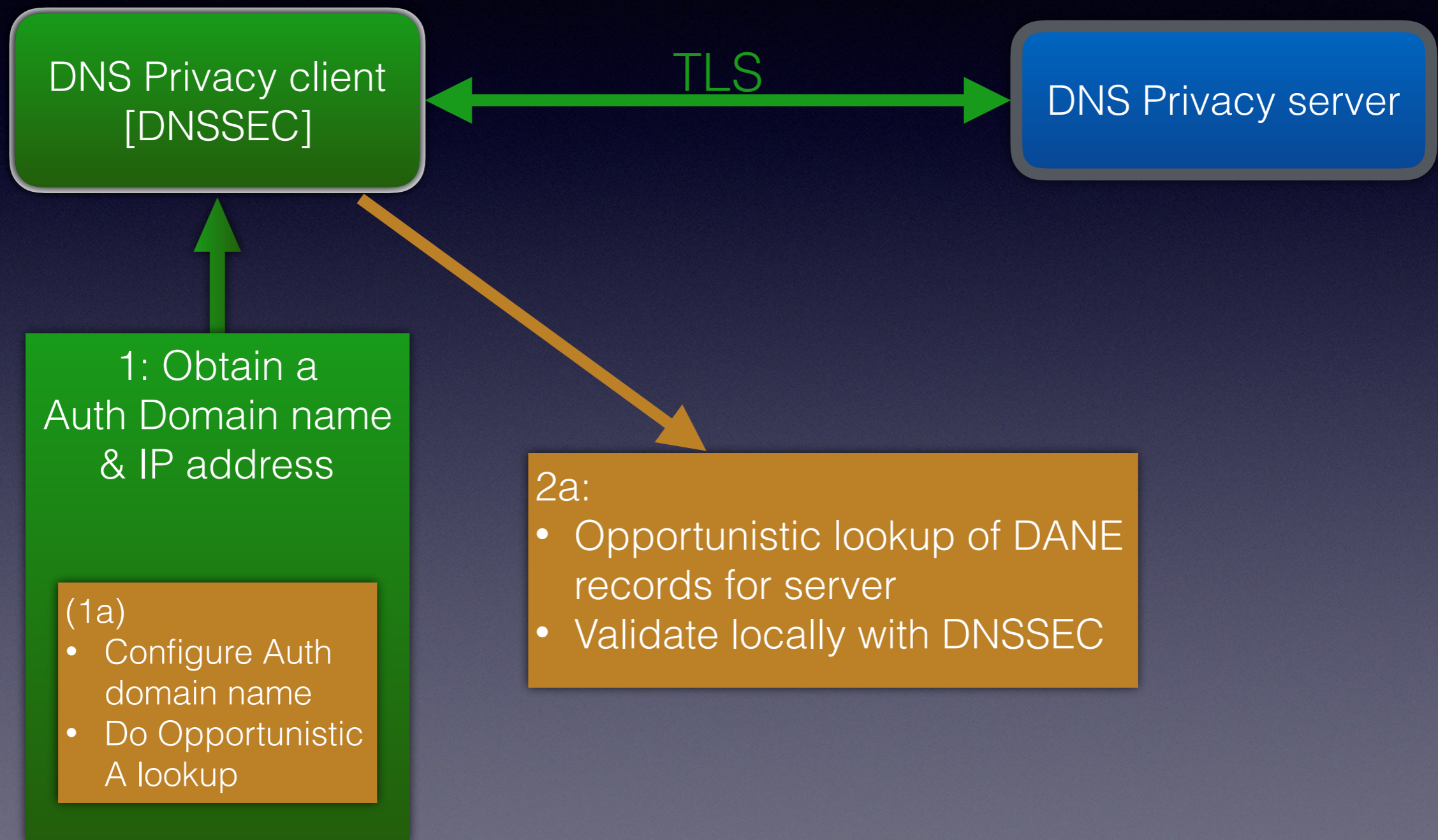
# DNS Auth using DANE



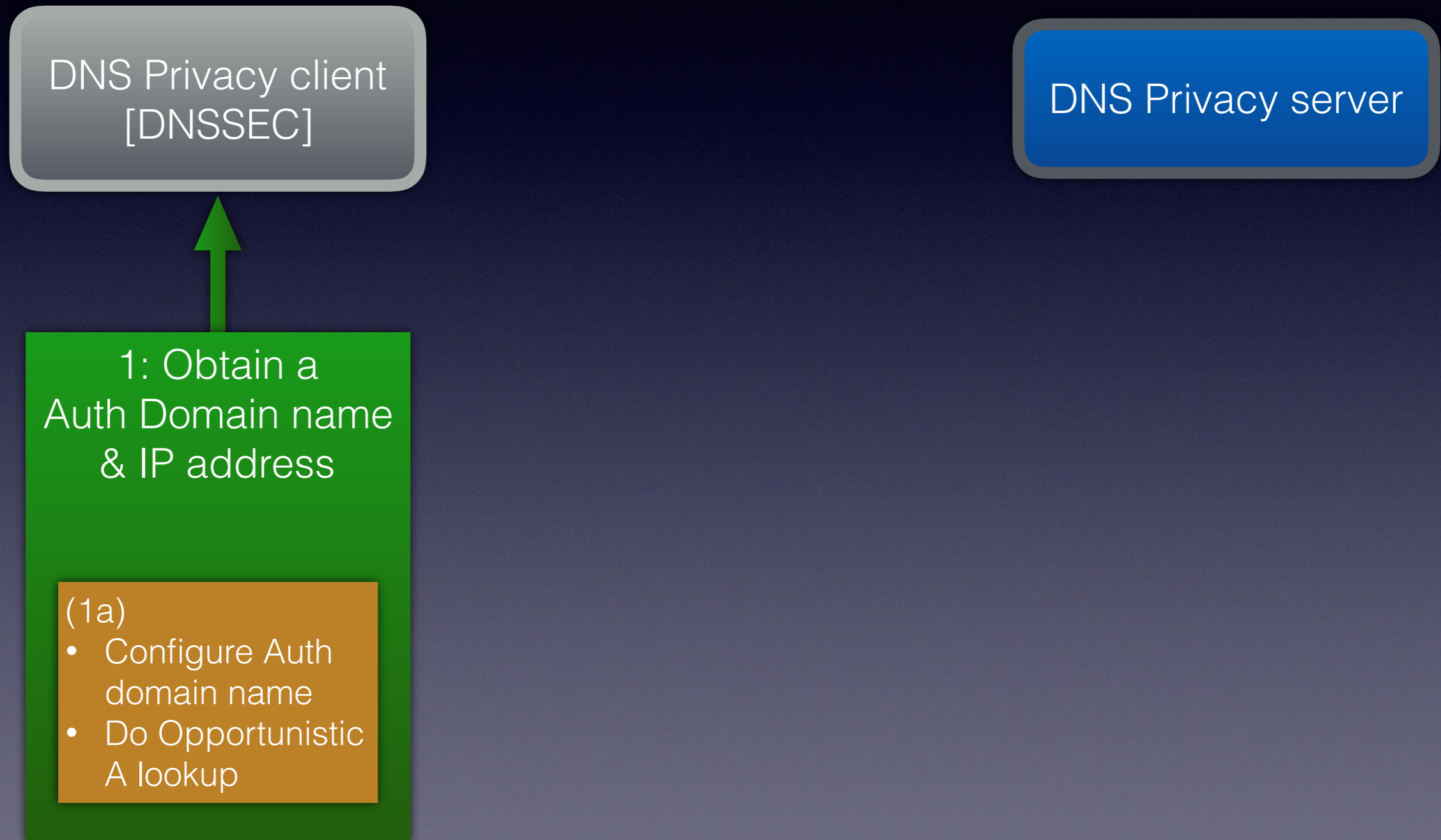
# DNS Auth using DANE



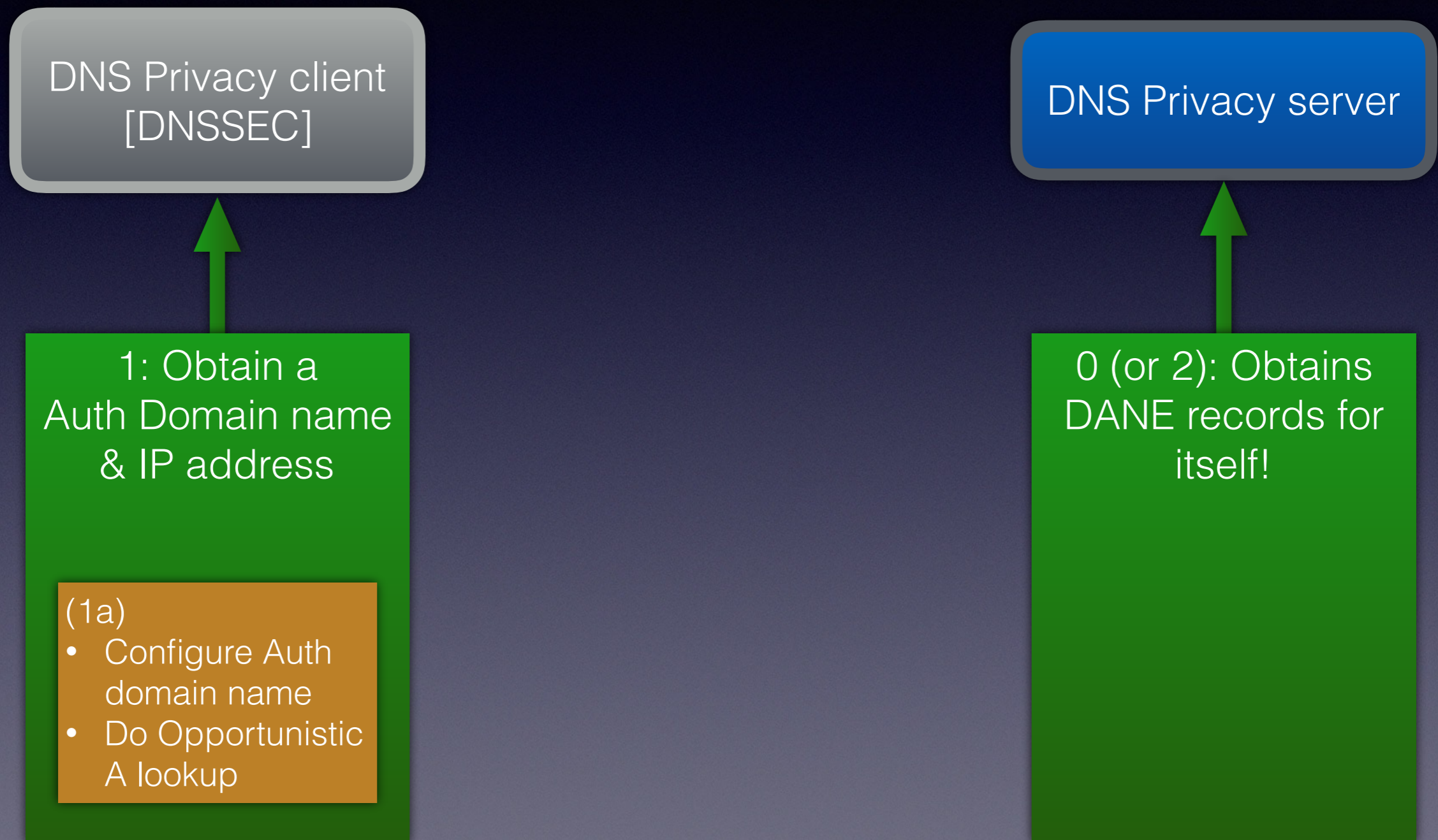
# DNS Auth using DANE



# TLS DNSSEC Chain Extension

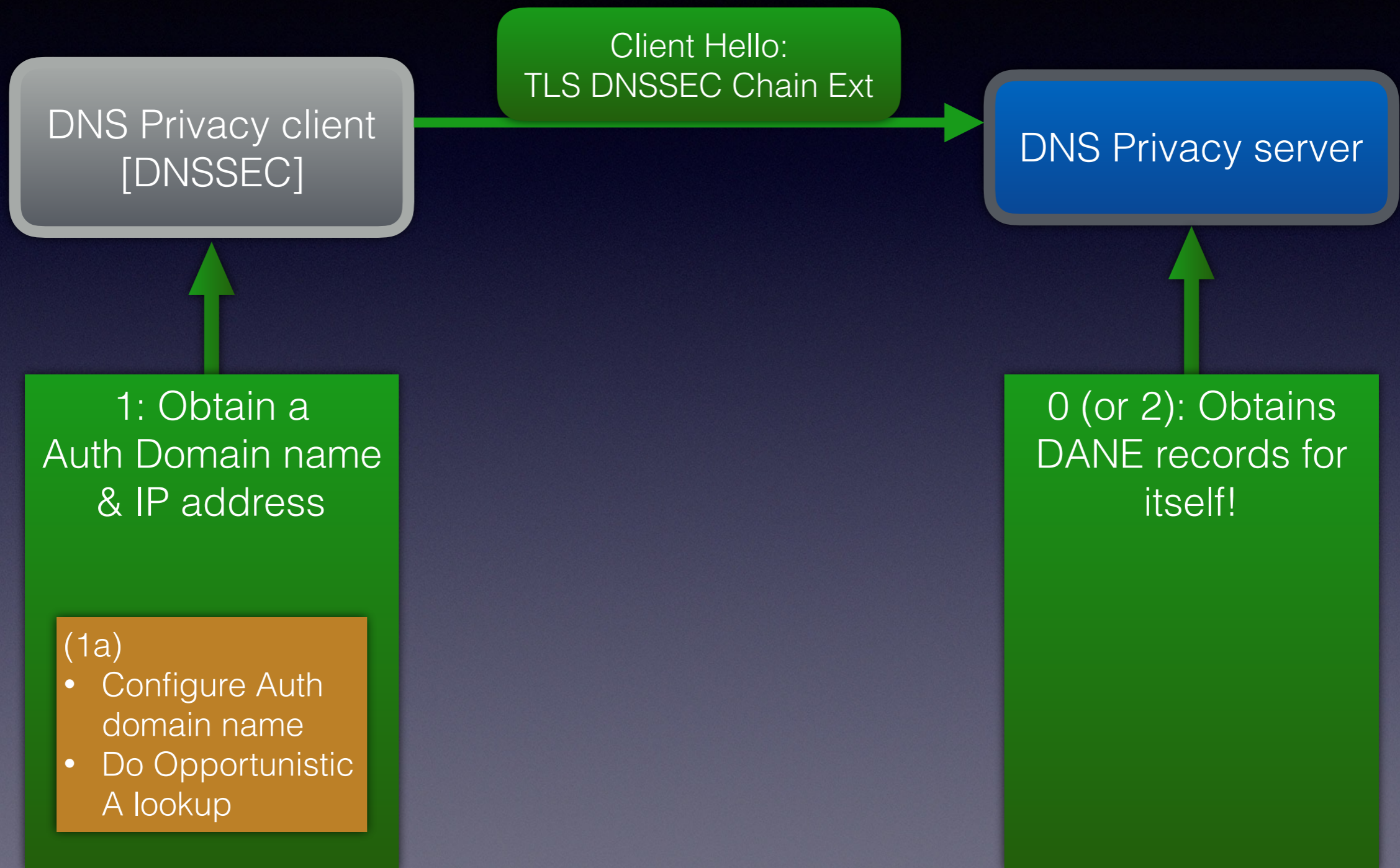


# TLS DNSSEC Chain Extension

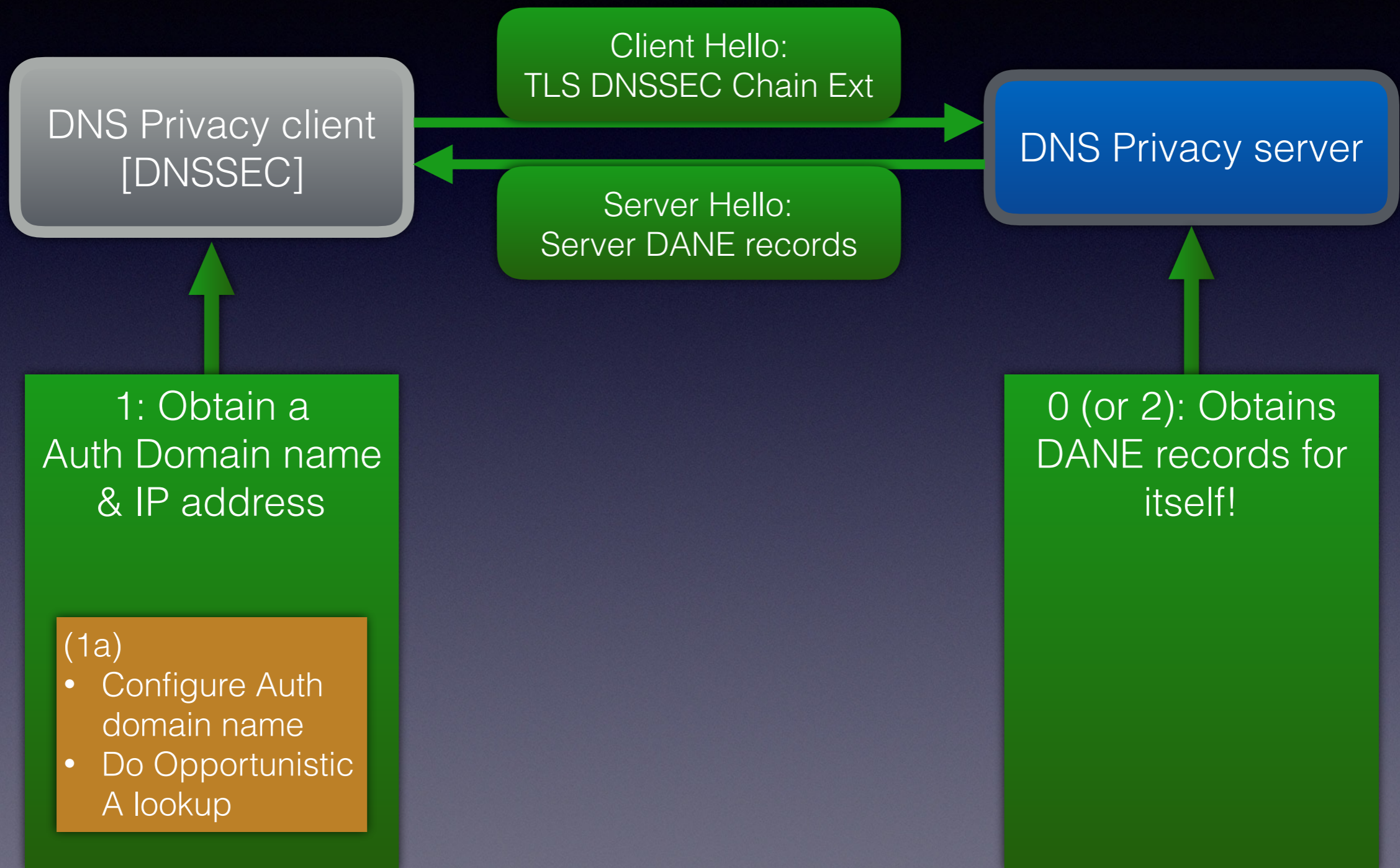




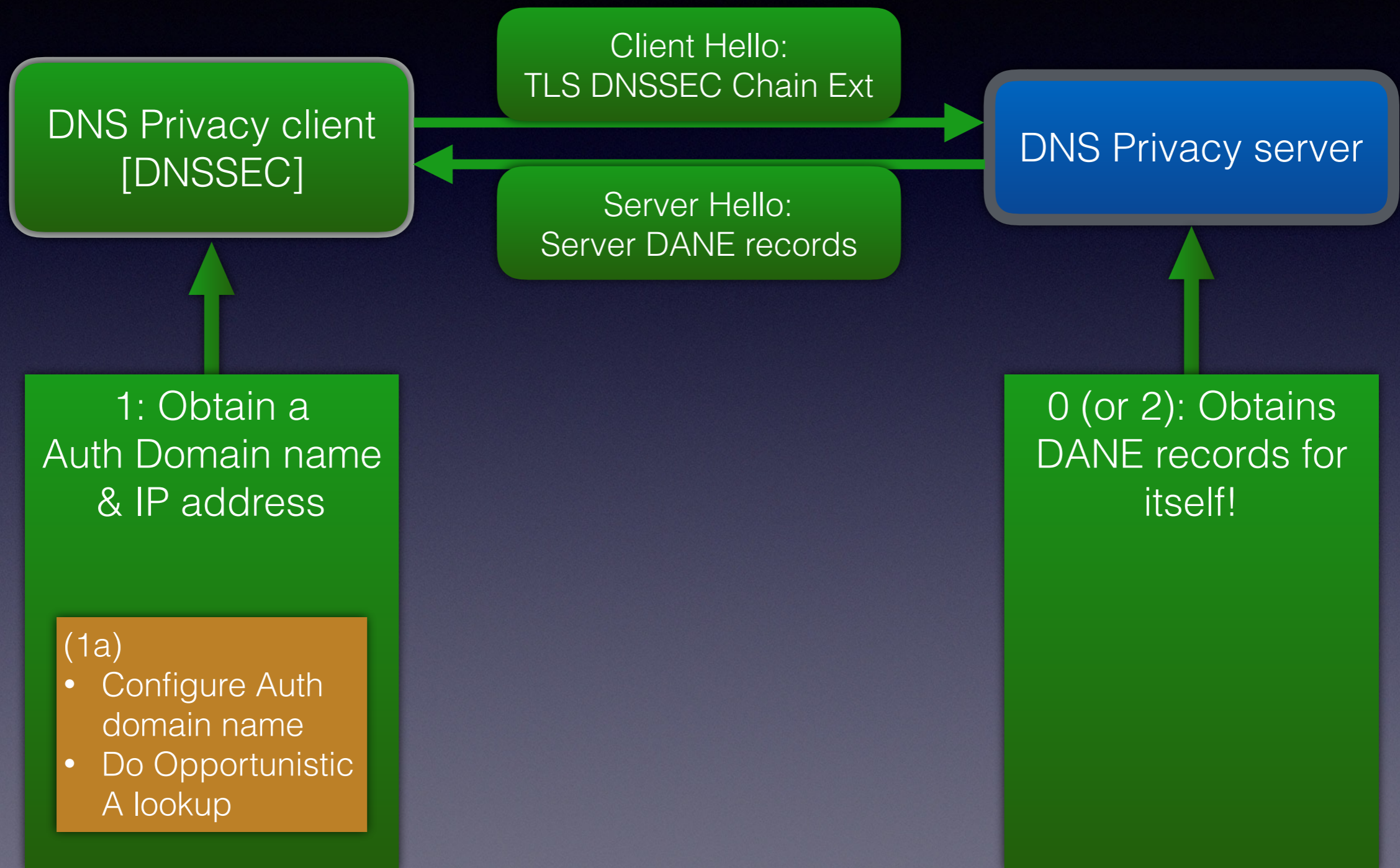
# TLS DNSSEC Chain Extension



# TLS DNSSEC Chain Extension



# TLS DNSSEC Chain Extension



# TLS DNSSEC Chain Extension

