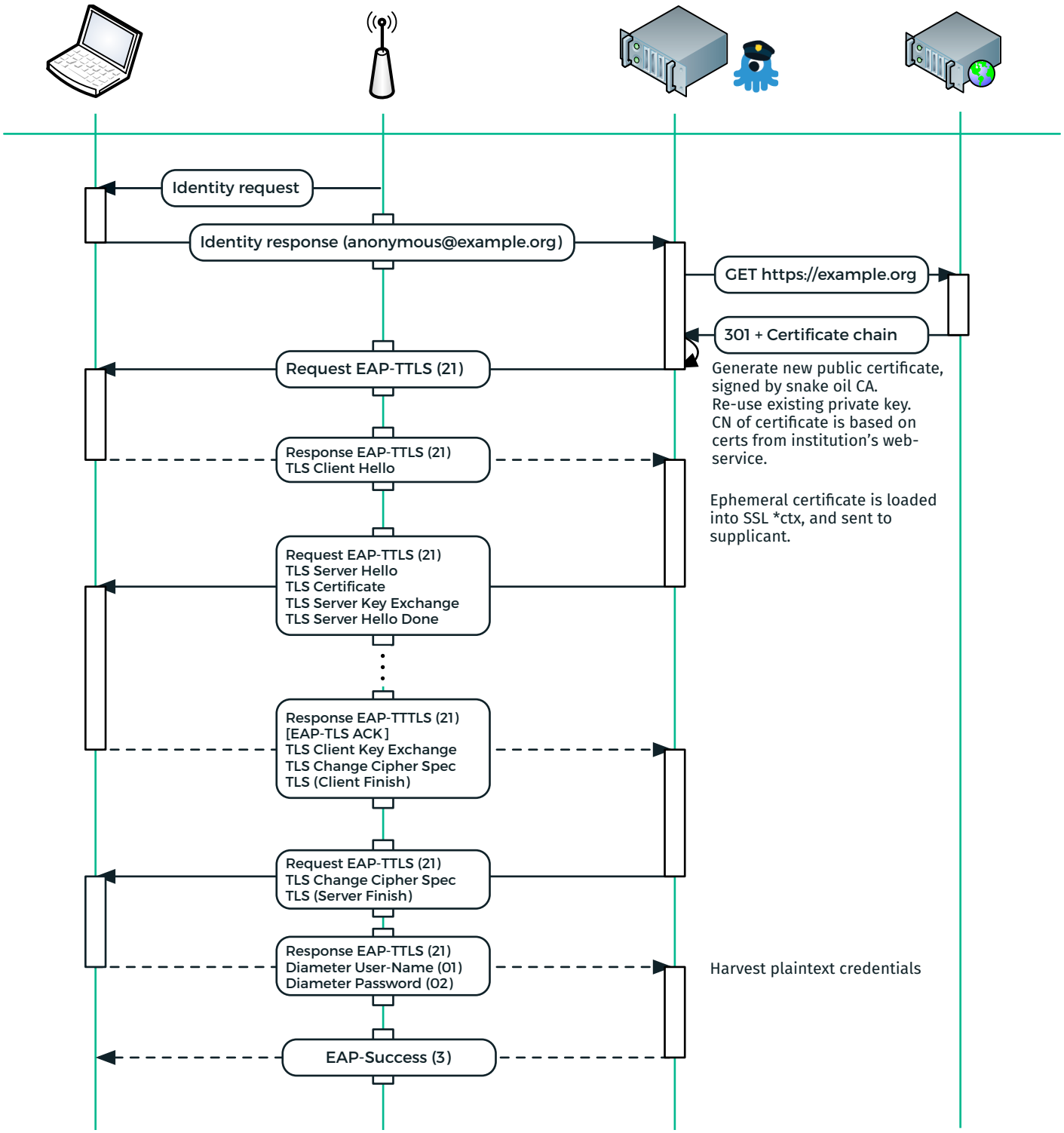
Identity request
Identity response (anonymous@example.org)
GET https://example.org
301 + Certificate chain
Generate new public certificate, signed by snake oil CA.
Re-use existing private key.
CN of certificate is based on certs from institution's web-service.
Request EAP-TTLS (21)
Response EAP-TTLS (21)
TLS Client Hello
Ephemeral certificate is loaded into SSL *ctx, and sent to supplicant.
Request EAP-TTLS (21)
TLS Server Hello
TLS Certificate
TLS Server Key Exchange
TLS Server Hello Done
Response EAP-TTTLS (21)
[EAP-TLS ACK]
TLS Client Key Exchange
TLS Change Cipher Spec
TLS (Client Finish)
Request EAP-TTLS (21)
TLS Change Cipher Spec
TLS (Server Finish)
Response EAP-TTLS (21)
Diameter User-Name (01)
Diameter Password (02)
Harvest plaintext credentials
EAP-Success (3)