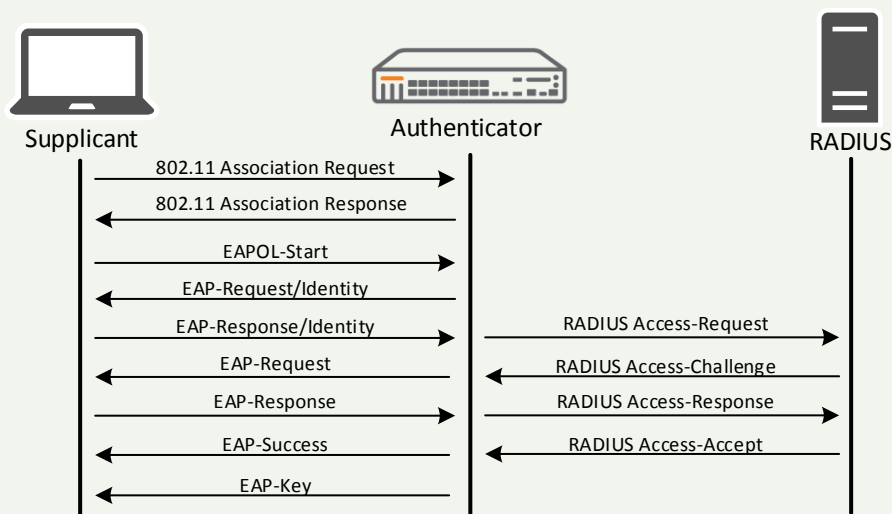


EAP Flow Overview



Useful OpenSSL Commands

Generate a new private key and Certificate Signing Request

```
openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -keyout privateKey.key
```

Convert a DER file (.crt .cer .der) to PEM

```
openssl x509 -inform der -in certificate.cer -out certificate.pem
```

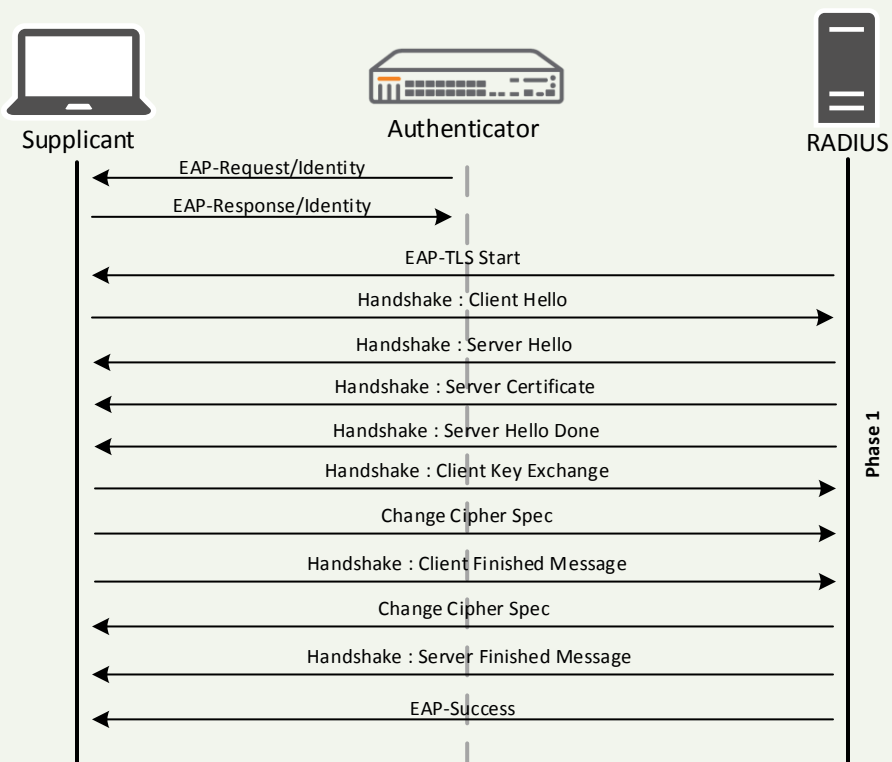
Convert a PEM file to DER

```
openssl x509 -outform der -in certificate.pem -out certificate.der
```

Convert a PEM certificate file and a private key to PKCS#12 (.pfx .p12)

```
openssl pkcs12 -export -out certificate.pfx -inkey privateKey.key -in certificate.crt -certfile CACert.crt
```

EAP-TLS Handshake



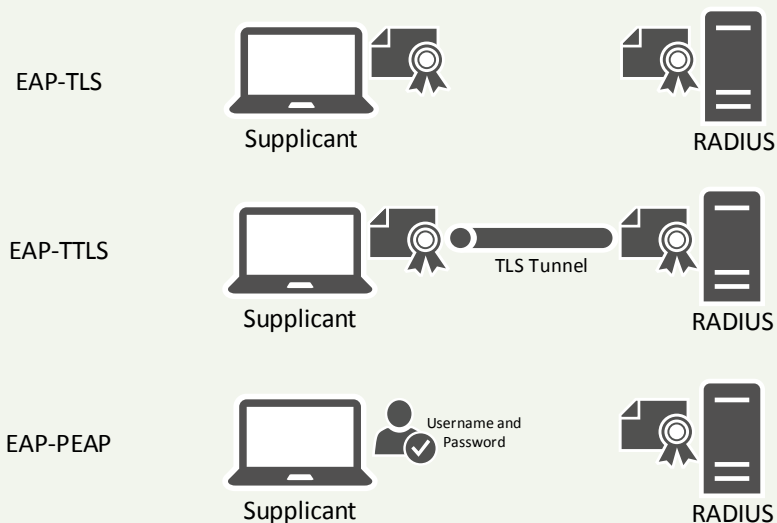
IETF RADIUS Dictionary (Most common attributes)

#	Attribute Name	ID	Type
27	Callback-Id	20	String
28	Callback-Number	19	String
29	Called-Station-Id	30	String
30	Calling-Station-Id	31	String
40	Egress-VLAN-Name	58	String
41	Egress-VLANID	56	Unsigned32
45	Filter-Id	11	String
50	Framed-IP-Address	8	IPv4Address
51	Framed-IP-Netmask	9	IPv4Address
57	Framed-Interface-Id	96	IfId
58	Framed-MTU	12	Unsigned32
59	Framed-Management	133	Unsigned32
64	Idle-Timeout	28	Unsigned32
82	Message-Authenticator	80	OctetArray
83	NAS-Filter-Rule	92	String
84	NAS-IP-Address	4	IPv4Address
85	NAS-IPv6-Address	95	IPv6Address
86	NAS-Identifier	32	String
87	NAS-Port	5	Unsigned32
88	NAS-Port-Id	87	String
89	NAS-Port-Type	61	Unsigned32
92	Password-Retry	75	Unsigned32
93	Port-Limit	62	Unsigned32
96	Reply-Message	18	String
99	Service-Type	6	Unsigned32
100	Session-Timeout	27	Unsigned32
101	State	24	OctetArray
103	Termination-Action	29	Unsigned32
107	Tunnel-Medium-Type	65	Unsigned32
110	Tunnel-Private-Group-Id	81	String
113	Tunnel-Type	64	Unsigned32
114	User-Name	1	String
115	User-Password	2	String
116	User-Priority-Table	59	OctetArray
117	Vendor-Specific	26	OctetArray

Aruba RADIUS Dictionary (Most common attributes)

#	Attribute Name	ID	Type
1	Aruba-AP-Group	10	String
2	Aruba-AP-IP-Address	34	IPv4Address
3	Aruba-AP-Name	13	String
6	Aruba-Admin-Path	42	String
7	Aruba-Admin-Role	4	String
8	Aruba-AirGroup-Device-Type	27	Unsigned32
9	Aruba-AirGroup-Shared-Group	35	String
10	Aruba-AirGroup-Shared-Role	26	String
11	Aruba-AirGroup-Shared-User	25	String
12	Aruba-AirGroup-User-Name	24	String
13	Aruba-AirGroup-Version	38	Unsigned32
16	Aruba-CPPM-Role	23	String
17	Aruba-Calea-Server-Ip	41	IPv4Address
18	Aruba-Device-Type	12	String
19	Aruba-Essid-Name	5	String
20	Aruba-Framed-IPv6-Address	11	String
21	Aruba-Location-Id	6	String
32	Aruba-Named-User-Vlan	9	String
35	Aruba-Port-Bounce-Host	40	Unsigned32
36	Aruba-Port-Id	7	String
39	Aruba-User-Group	36	String
40	Aruba-User-Role	1	String
41	Aruba-User-Vlan	2	Unsigned32

Common 802.1x Authentication Methods



Common RADIUS Ports

UDP/1812 : Authentication and Authorization port
 UDP/1813 : Accounting port
 UDP/3799 : COA (RFC 3576)

EAP Codes

1	Request
2	Response
3	Success
4	Failure

RADIUS Service-Type

Number	Description
1	Login
2	Framed
3	Callback Login
4	Callback Framed
5	Outbound
6	Administrative
7	NAS Prompt
8	Authenticate Only
9	Callback NAS Prompt
10	Call Check
11	Callback Administrative
12	Voice
13	Fax
14	Modem Relay
15	IAPP-Register
16	IAPP-AP-Check
17	Authorize Only
18	Framed-Management
19	Additional-Authorization

RADIUS Port-Type

Number	Description
0	Async
1	Sync
2	ISDN Sync
3	ISDN Async V.120
4	ISDN Async V.110
5	Virtual
6	PIAFS
7	HDLC Clear Channel
8	X.25
9	X.75
10	G.3 Fax
11	SDSL - Symmetric DSL
12	ADSL-CAP - Asymmetric DSL
13	ADSL-DMT - Asymmetric DSL
14	IDSL - ISDN Digital Subscriber Line
15	Ethernet
16	xDSL - Digital Subscriber Line of unknown type
17	Cable
18	Wireless - Other
19	Wireless - IEEE 802.11

Useful SQL Commands

QUERYING A TABLE

SELECT c1, c2 FROM t;
 Query data in columns c1. c2 from a table

SELECT * FROM t;
 Query all rows and columns from a table

SELECT c1, c2 FROM t;
WHERE condition;
 Query data and filter With a condition

SELECT DISTINCT c1 FROM t;
WHERE condition;
 Query distinct rows from a table

SELECT c1, c2 FROM t;
ORDER BY c1 ASC [DESC];
 Sort the result set in ascending or descending order