Fact Sheet

Cogito Group

802.1X EAP-TLS

What is 802.1X?

The 802.1X protocol is a network access control standard that ensures secure authentication of devices before granting access to a network. It operates as part of the IEEE family of standards and is commonly used in wired and wireless networks.

The 3 key components of 802.1X are:

1. Supplicant
   - The client device (laptop, computer, smartphone) seeking network/internet access.
2. Authenticator
   - The gatekeeper device (WiFi access point, network switch) allows or blocks the client connection based on the response from the server.
3. Server
   - The RADIUS (Remote Authentication Dial-In User Service) server validates the client's credentials and Accept or Rejects the authentication.

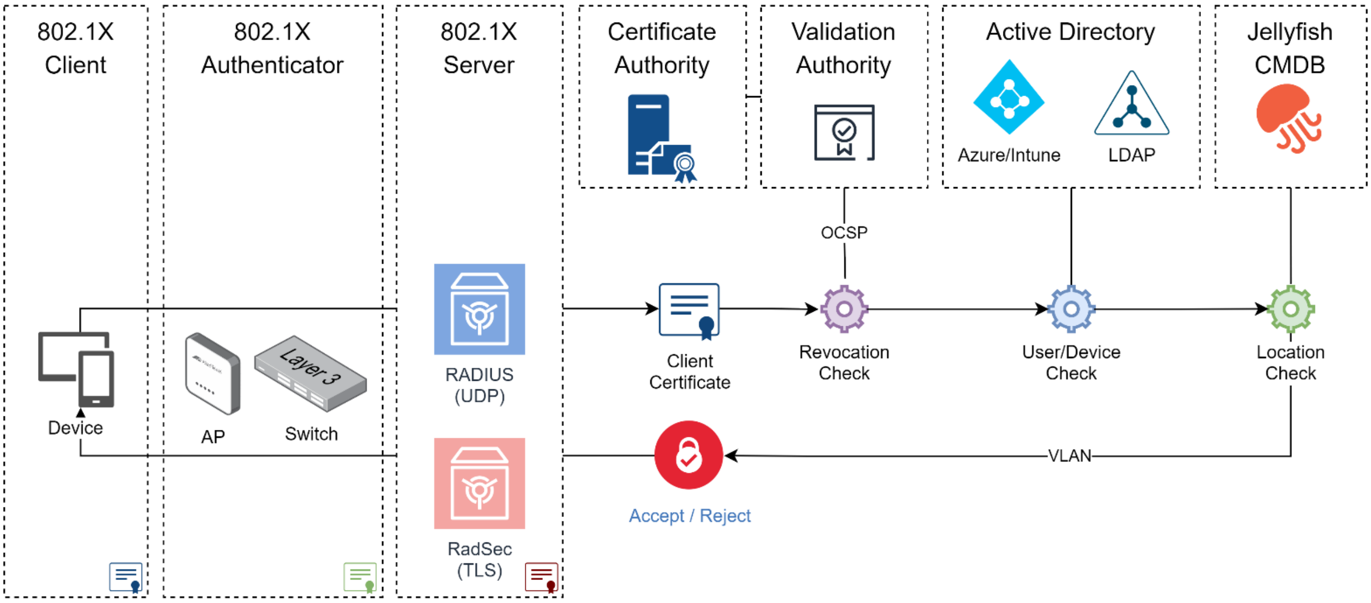
802.1X Authentication Methods:

• EAP-TLS:	Uses x509 Certificates on both the client and server for mTLS.
• EAP-TTLS/PEAP:	Tunnel other EAP methods via server x509 Certificate.
• MSCHAPv2:	Uses username + password on client.
• EAP-PWD:	Uses username + password on client.
• EAP-MD5	Uses password on client.

802.1X EAP-TLS

Fact Sheet

Jellyfish 802.1X Workflow



What is EAP-TLS?

EAP-TLS is the most secure and one of the most widely used 802.1X EAP authentication method. It uses x509 Certificates on both the client and server to establish mutual between the client device and RADIUS server. The mutual authentication makes it immune against many attack vectors present in password-based authentication, since both client and server can verify each other's identity.

Advantages of EAP-TLS:

• Strong Security:	Certificates are more secure than passwords.
• Encryption:	All communication between client and server is encrypted.
• Compliance:	Meets the most stringent data protection standards.

What is RadSec?

RadSec (RADIUS over TLS) is an optional security enhancement to the 802.1X standard enabling encryption between the Authenticator (access point, network switch) and the RADIUS Server.

In EAP-TLS all communication between the Client Device and RADIUS Server are encrypted, however the intermediary Authenticator's communication to the Server remains unencrypted. A pre-shared key does exist between the Authenticator and Server, but it is only used for initial authentication and checksum of follow up messages.

RadSec secures the connection between the Authenticator and Server, replacing the UDP connection with an encrypted Certificate based TCP connection.

802.1X EAP-TLS

Fact Sheet

Jellyfish 802.1X EAP-TLS

Jellyfish is a x509 Certificates management platform enabling certificate issuance through Web Portal, SCEP, Autoenrollment and ACME. As a certificate provider Jellyfish equips clients and servers with certificates which can be used to enable 802.1X EAP-TLS authentication for your network. The Jellyfish platform also hosts custom EAP-TLS RADIUS and RadSec servers with additional capabilities enabling User/Device verification, Shared Accommodation, location-based statistics and reporting.

Private RADIUS Server

Organisations can issue a server certificate from Jellyfish platform and host their own 802.1X RADIUS server. Clients within the organisation can then enrol Client certificates through Intune to authentication to corporate network. Typically, organisations host an additional guest WiFi network to enable client devices to enrol the authentication certificate and then once the client has the certificate they switch to the corporate network. Alternatively, system administrators can install the authentication certificate manually during device build process and rely on autoenrollment to renew the certificate.

Jellyfish RADIUS Server

The Jellyfish RADIUS/RadSec Cloud solution removes the complexity of hosting RADIUS server within your environment. All EAP-TLS authentications are validated, revocation checked and authorized on a certificate level. Connections to Jellyfish can be established with RadSec or RADIUS over IPSec VPN tunnel.

- LDAP / Azure Authentication

Jellyfish has developed an enhanced EAP-TLS authentication verifying the user/device details in the x509 Certificate with LDAP/Azure. This enables organisation to control WiFi and network access on a user level.

- Smart Resources

Jellyfish Smart Resources enables multiple scenarios that need combined data. An example is support for multiple organisations shareing the same physical network. It places individual user/devices on the correct VLAN network based on the client Certificate, but can provide a number of other capability related to Visitor Management, Turnstile and Physical Access Control, Printer access, Locker access, etc. More information can be found in our Smart Resources web page.

- Statistics

Jellyfish Capacity Dashboard enables location-based statistics for enabling live view of building, floor and zone utilization based on RADIUS access point authentication or accounting data.

- Reporting

Jellyfish Reporting enables details reports for zone-based authentications for your organisation. This optionally includes contact tracing and meeting room utilisation.

802.1X EAP-TLS

Fact Sheet

The client devices authenticate with x509 Certificates to the RADIUS/RadSec server. During this authentication both client and server present their certificates, and they verify each other. Next the server preforms additional revocation checking, user/device lookup and location lookup. If everything verifies the server returns the VLAN tag and Request Accept response and the Switch/Access Point authorizes the client connection to the network.

Comparison

	Private 802.1X	**Jellyfish 802.1X**
Server Connection	RADIUS	RadSec, RADIUS + VPN
Server Location	On-Premises	Cloud/On premises
Authentication	Certificate	Certificate + User + Location
Revocation Status	-	OCSP Check
Rich Service Support	-	Allows support of contact tracing, smart resourcing and usage statistics reporting.

About Cogito Group

Cogito Group is an award-winning, Australian owned and operated ICT company, specialising in authentication, cloud security, identity management and data protection. Cogito Group protect the authentication methods used to access information through the use of Identity and other security technologies. Cogito Group protect data not only from unauthorised access and disclosure, but also from being altered by an unauthorised third party or a trusted insider with malicious intent. This assists in the detection and prevention of fraud or other malicious activities by third parties or trusted insiders.