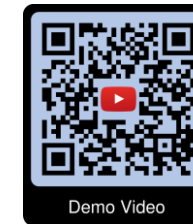


802.1x comes with added benefits of Policy enforcement adding an additional layer of security and limiting lateral movement.



- ## References
1. A. Purcell, "3 key ideas to help drive compliance in the cloud", IBM, 2018
<https://www.ibm.com/blogs/cloud-computing/2018/01/16/drive-compliance-cloud/>
accessed 20/07/2022
 2. "Planning for a Zero Trust Architecture: A planning guide for federal administrators" White Paper, NIST CSWP 20, <https://csrc.nist.gov/publications/detail/white-paper/2022/05/06/planning-for-a-zero-trust-architecture/final> accessed 20/07/2022
 3. Wired 802.1x Deployment Guide, https://www.cisco.com/c/en/us/rd/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html accessed 15/07/2022.

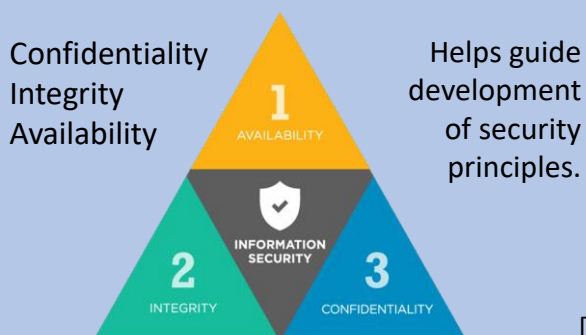
EAP-TLS

Requires PKI – Public Key Infrastructure

Easier to configure

Mutual Authentication. Re-assures the device that the network it is joining is genuine. Mitigates man-in-the-middle attacks.

Each letter represents a foundational principle. When all 3 standards are met, security posture is stronger.



Simplified authentication flow process

4. If PEAP-MSCHAPv2, supplicant responds containing its credentials to the or EAP-TLS, sends device certificate to Authenticator.

3. Credentials used to identify device. Policy sets are pushed to NAD to enforce policies on Supplicant discretionary Access Control List (dACL).

2. Authentication Server can use Group membership in Policy Sets to limit access.

Principles include, segmentation, authentication, threat protection and granular least access policies. [21]

