

Deploying Wi-Fi Asset Tags – Frequently Asked Questions

Q1: What's the advantage of using Telemetry over EAP?

To answer this it is important to understand the alternative options. One option is to allow the tag guest access to the corporate network, allowing the tag to transmit its telemetry information via UDP or TCP packets across the Internet to a telemetry server (G2 Tag Engine) configured to receive the telemetry data.

The issues with this approach are:

- The tag needs to know the access credentials to access the guest network. Guest access configuration can vary at each node necessitating that the tag knows access information for every node that it might visit. Even worse, problems arise if nodes change their access credentials after tags are already deployed.
- Even if the tag can be protected by using guest VLANs, enterprises are generally wary of these techniques. Concerns occur around the trustworthiness of the VLAN implementation and correct VLAN configuration.
- While wireless security features like WPA2 might be enabled, this only protects the wireless segment. Unless encryption is applied at the data payload level, the contents of the transmitted data are not protected over the Internet.

In comparison Telemetry over EAP provides the following benefits:

- The tag is never granted access on the corporate data network.
- Configuration of the RADIUS server is 'one time' prior to tag deployment.
- Because no secret pre-shared keys are used, there are no issues with key management for each node.
- The tag does not need to carry separate security credentials for each node in order to access that node, therefore a tag always knows how to send data.
- Mutual server-tag authentication uses certificates, hence it is not possible to receive information from a fake tag.
- All information between the tag and the receiving RADIUS server is sent through an encrypted tunnel. This prevents man-in-the-middle (Mitm) attacks.
- Because certificates form the basis of authentication, tags can be disabled by simply revoking certificates and therefore theft of one tag does not compromise security for any other tag.

Q2: Will Telemetry over EAP overburden my RADIUS server and the WLAN controller or AP?

When a tag arrives at a node it sends its information through the WLAN AP and to the local RADIUS server. Because the RADIUS server is providing a proxy service it has minimal computing overhead and can handle a lot of requests. Similarly, the AP is merely passing through the requests and responses and does not have to process a great deal of information. Because the tag always receives an acknowledgment, the amount of traffic can be limited to a single send per tag per node. Typical tag data payloads might be 500 bytes, e.g. arrival timestamp plus the log of collected temperature data. To this, we add the cost of setting up the EAP connection.

When using session resumption, the total traffic between the tag and the local RADIUS server to create a connection is approximately 1KB and requires an exchange of around eight small packets in total, i.e. four in each direction. Per tag message, the total traffic is in the range 100 to 250 bytes per message. This is low enough to have negligible impact on the network. Tag telemetry data could then be another 500 bytes in one of these packets depending on the application.

Q3: Does proxying the RADIUS server mean that I have to expose my RADIUS server to the Internet?

Yes and no. Because a node's RADIUS server is initiating all transactions, the exposure is no worse than that of a corporate laptop using a web browser to connect to an external server. The corporate firewall needs to allow the local RADIUS server to initiate a connection to the receiving RADIUS server. The firewall can be easily configured via ACLs to ensure that the RADIUS server is not exposed to attack.

The receiving RADIUS server (tag owner's), needs to be able to receive connections and is therefore exposed to the Internet and potentially subject to attack. There are a number of actions that can be taken to limit this risk:

- Make the tag RADIUS server independent of the corporate users' RADIUS server, limiting any vulnerability.
- Configure the incoming firewall to limit connections to the known RADIUS servers of the nodes that will make a connection.
- Secure the RADIUS server connections with a strong shared secret.
- Place the connection between the RADIUS servers inside a virtual private network (VPN) connection.
- Use an Internet-hosted service as proposed for proof-of-concept trials.

Q4: Can you guarantee that a tag is never granted access to my corporate data network?

Yes. One of the benefits of Telemetry over EAP is that the tag is never granted access to the data network. Traffic is carried only on that part of the network that checks and guarantees corporate network security. So regardless of whether the tag is trusted or whether there is a rogue device pretending to be a tag, access to the data network is never granted.

Please see document "G2 Microsystems - Enabling Wi-Fi Asset Tags in a Supply Chain" for further details. Q5: What happens if I do not have RADIUS infrastructure support at the supply chain node? You have a number of choices which have varying security considerations.

- One alternative is to configure a SSID for 802.1x authentication on the local WLAN controller or AP for which the RADIUS server is the tag owner's RADIUS server. This allows Telemetry over EAP to operate without a local proxy RADIUS server. It is preferable to also have a VPN between the WLAN controller or AP and remote RADIUS server to hide identity information flowing across the Internet.
- Another alternative is to allow the tag access to the local wireless network and to communicate with the remote telemetry server via UDP, but this has the disadvantages outlined in question 1.

Q6: Am I protected from Denial of Service (DoS) attacks?

Denial of Service attacks can be made on any wireless network at a supply chain node. Implementing Telemetry over EAP neither increases nor decreases the possibility or risk of DoS attacks. A Cisco Systems® WLAN network provides various mechanisms for mitigating DoS attacks.

Q7: Have major network and security vendors reviewed the Telemetry over EAP approach?

Yes, G2 is working very closely with Cisco Systems to vet the security implications of Telemetry over EAP.

The Cisco Secure Wireless Solution infrastructure will support both EAP-TLS/TAG and EAP-FAST/TAG at the supply chain node.

The Cisco Secure Wireless Solution infrastructure will support EAP-FAST/TAG at the tag owner's site to receive telemetry information.

Please refer to the document titled "*Cisco Secure Wireless Solutions*".

Telemetry over EAP was created in collaboration with XEROX PARC, one of the world's premier computer science and security research labs.

Q8: EAP-TLS and EAP-FAST need certificates. How are certificates deployed in tags?

Contrary to common concerns, certificate management is fairly simple. The first thing to note is that supply chain nodes do not need to know anything about a tag's certificate or how they are managed. All certificate handling is transparent to the supply chain node.

In summary:

- A Certificate Authority (CA) software application creates private keys and signed public certificates for the tags, and inserts these unique certificates into the tag when the tag is provisioned for deployment.
- The tag owner's RADIUS server is given a copy of the CA's own unique public key as part of the CA certificate. It's no more complicated than giving the tag its identity and other information that it needs to be useful.

In more detail:

When a tag is 'birthed' it is given an Ethernet MAC address and other information. At this point, it is provided private and public keys unique to the tag. The tag's public key is signed by the private key Certificate Authority (CA) that issues the tag's certificate. The certificate authority (a software application) does not have to be a public CA like Verisign, it can be — and usually is — a CA run by the tag owner.

The RADIUS server is given the public key of the CA. When the tag makes an EAP-TLS or EAP-FAST connection with the RADIUS server, the RADIUS server uses the fact that the CA signed the tag's public certificate to verify any information signed by the tag using the tag's private key.

Q9: What information is exposed to the Internet and what is encrypted?

For a tunneled EAP method based on EAP-TLS, such as EAP-TLS/TAG or EAP-FAST/TAG, an encrypted TLS tunnel is set up between the endpoints of the RADIUS server and client (tag) This is opaque to all intermediaries including the WLAN controller or AP. The client is then able to send data through the encrypted tunnel as TLS application data. Encryption takes place at the TLS layer and not at the 802.11 MAC layer so no other 802.11 encryption is needed.

In Telemetry over EAP, an enterprise-level RADIUS server is configured to act as a proxy and forward requests to other RADIUS servers. This is done on the basis of the user name supplied in the response to an identity request. For example, a tag client username could be tag_client@tag.g2microsystems. The part of the username after the @ sign is called a realm. Authentication requests with a realm of tag.g2microsystems can be configured on the local RADIUS server to be forwarded to a remote RADIUS server while all other requests are handled locally. To protect some of this 'identity information' before the TLS tunnel connection is made, the RADIUS-to-RADIUS connection should be protected with a VPN between the proxy Radius server and the tag owner's RADIUS server. Since it is only identity information, some may not choose to use a VPN connection.

The identity information sent over the wireless, between the tag and WLAN controller or AP prior to tunnel setup, can only be protected by having an EAP inner method such as that allowed by EAP-FAST or PEAP, i.e. it is a higher grade of security which will be available with EAP-FAST/TAG and EAP-PEAP/TAG. Again, it is identity information only; telemetry data is not exposed.

Q10: What other EAP methods do you support?

In 2007, G2 will be supporting Telemetry over EAP methods based on EAP-TLS and EAP-FAST. These are known as EAP-TLS/TAG and EAP-FAST/TAG. Both EAP-TLS/TAG and EAP-FAST/TAG support is available in the Cisco Secure Access Control Servers (ACS) and should be the preferred choice for production deployments.

It is important to note that RADIUS servers at the node do not have to support any of these methods; they simply have to be able to provide proxy support. Most commercial RADIUS servers can provide this functionality. Only RADIUS servers at the tag owner's end need to understand the specifics of Telemetry over EAP.

In 2008, G2 may add support for EAP-PEAP. This extension will be known as EAP-PEAP/TAG.

1475 S. Bascom, Suite 109
Campbell, CA 95008
Phone: +1-408-626-4812
Email: info@g2microsystems.com
www.g2microsystems.com

