Cylentium Architecture

CYLENTIUM White Paper

This document describes the architecture and internals of Cylentium Technology, with responses to question posed by the Joint Systems Integration Command (JSIC) USJFCOM

Rev 1.2
03/30/2020

Contents

Acronyms

AES	Advanced Encryption Standard
CA	Certificate Authority
COTS	Commercial Off the Shelf
DES	Data Encryption Standard
EAP	Extensible Authentication Protocol
FIPS	Federal Information Processing Standard
HIPAA	Health Insurance Portability and Authorization Act
HMAC	Hashed Message Authentication Code
LDAP	Lightweight Directory Access Protocol
OSI	Open Systems Interconnect
PKI	Public Key Infrastructure
PMS	Pre-Master Secret
RADIUS	Remote Authentication Dial-In User Service
SHA	Secure Hash Algorithm
TTLS	Tunneled Transport Layer Security
TLS	Transport Layer Security
VLAN	Virtual Local Access Network
WAC	Cylentium Zero Identity Access Controller
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Introduction

Cylentium Zero Identity is the industry's premier FIPS 140-2 validated software-based solution for protecting wireless networks at Layer 2 of the OSI model. Based on an open, non-proprietary architecture, the system extends existing Wi-Fi component-level standards to solve specific system-level issues. Cylentium Zero Identity provides a tightly integrated framework enabling interoperability with existing identity management, policy, and security applications while providing broad-based support for a wide variety of wireless, ethernet, and network devices. The system runs on standard, commercially available[1] off-the-shelf (COTS) hardware. As Cylentium Zero Identity is **independent of the type of radio technology being deployed,** the system can support any mix of 802.11a, b, g, j, or n access points from any vendor, and supports newer 802.11 standards like 802.11n, and operating across long-haul bridges such as 802.16 (WiMAX). The architecture fulfills five objectives:

1. It enforces uniform high (WPA2-Enterprise) security-only across heterogeneous networks.

2. Allows wide strategic options of deployment and coverage from simple segmentation, to deep micro-segmentation

3. It protects existing infrastructure investment by enabling strong security on legacy devices which may not support WPA2-Enterprise mode.

4. It improves end-to-end security by extending encryption from the client to the data center instead of at the access point, which may otherwise leave the distant bridge from datacenter to AP vulnerable.

5. It centralizes firewall and port-management policies for large clusters of access points, simplifying management that would otherwise have to be replicated to each access point.

Cylentium Zero Identity has three main components as shown in Figure 1:

Cylentium Zero Identity Manager – The Cylentium Zero Identity Manager is a secure browser-based application providing centralized configuration, monitoring, and management of the secure wireless network. The Manager utilizes credentials and group information stored in existing enterprise identity management systems (e.g., Active Directory, LDAP, RADIUS, Kerberos, and other management systems) for authentication, authorization, and policy selection.

Cylentium Zero Identity Access Controller – The Cylentium Zero Identity Access Controller (WAC) allows enterprises to integrate wireless users into their wired LAN architecture and enforces all policies created on the Cylentium Zero Identity Manager. The WAC runs on COTS hardware and physically separates the wireless network from the wired network. Acting as the gatekeeper to the wireless network, Cylentium Zero Identity enforces all policies created on the Manager and performs all session management tasks

[1] DELL, HP, CISCO, Aruba, Checkpoint, Extreme,

required for secure wireless LAN operation, including secure authentication tunneling, data encryption and decryption, firewall filtering, and mobility services.

Cylentium Zero Identity Client – The Cylentium Zero Identity Client is a zero-configuration thin client that runs on each Cylentium Zero Identity-enabled mobile device connected to the wireless network. The Client communicates with the Cylentium Zero Identity Access Controller to ensure secure authentication, to encrypt and decrypt wireless traffic. The Client incorporates a simple, easy-to-use interface for both login and for cryptographic bypass, for use when a Cylentium Zero Identity infrastructure is not available.   The client is available for Windows from Windows 98 to Windows 10, MacOS, iOS, Android OS, Linux 2.4 to 2.6 kernels, and Windows CE.

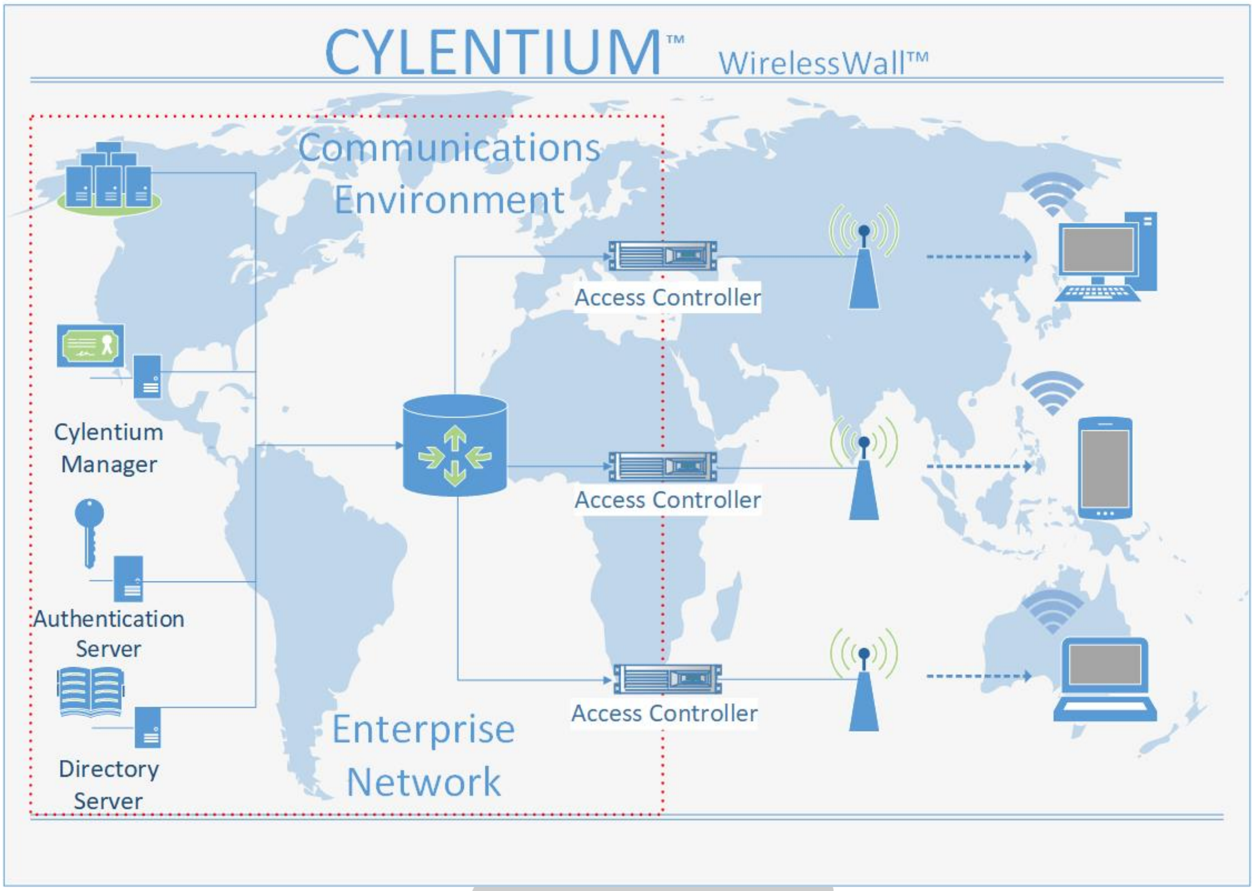

Figure 1: Cylentium Zero Identity reference architecture

Easy Integration with Existing Network Infrastructure

Cylentium Zero Identity is designed to integrate with existing wired switching/routing infrastructure as an overlay, minimizing the need for reconfiguration of the wired network. Enterprise networks and enterprise-grade access points are typically carrying different classifications of traffic over different VLANs. Cylentium Zero Identity supports VLAN tagging, providing network architects significant flexibility in the integration of wireless into existing wired networks by using VLAN trunks.

Cylentium Zero Identity provides significant capability for high availability. Cylentium Zero Identity Access Controllers can be used in parallel to provide hot standby. As the WAC is a software application on COTS hardware, the cost to deploy redundant systems is significantly lower than using proprietary hardware appliances. Cylentium Zero Identity provides local directory caching—a significant capability for large enterprises, where communication with enterprise directories may be lost from time to time. Using local directory caching Cylentium Zero Identity maintains an updated local copy of the directory at the Cylentium Zero Identity Manager; if communication between the Manager and the enterprise directory is lost, users can still be authorized to use the wireless network. Directory caching also speeds the user authorization process, ensuring a smooth login process for authorized users.

The Cylentium Zero Identity Client also provides a powerful unified login option. In typical FIPS-certified solutions, a user logs into the local machine using cached credentials, then logs into the wireless network using domain credentials. While efficient from a security standpoint, two logins mean two challenges to the user. First, a user must log in twice, which is inconvenient. More importantly, two logins mean that administrator-defined login scripts do not run at the time of attachment to the network, preventing the download of virus updates, software patches, etc. Cylentium Zero Identity clients using unified login enjoy wireless network and domain authentication with a single login, ensuring execution of login scripts and further mitigating risk.

Role-Based Access Control and Policy Enforcement

A powerful feature of Cylentium Zero Identity is its ability to enforce policies unique to each connection, including a policy allowing guest Internet access, enabling administrators to deliver differentiated services to mobile users on the same network infrastructure. For example, the role-based firewall can limit traffic to a specific server while simultaneously allowing otherwise broad access to an authenticated mobile user. This capability creates new opportunities for creative network design and infrastructure cost savings. Role-based policy enforcement is also useful to permit guest access while protecting the enterprise network from unauthorized access.

Cylentium Zero Identity implements its role-based firewall with robust policy capabilities based on highly granular network traffic filtering. A simple secure browser-based dashboard allows security and network administrators to associate security policies with specific connections based on each user’s existing group/domain associations as defined by the enterprise’s directory service.

Cylentium Zero Identity provides multiple parameters for policy editing and enforcement, including Membership, Per-frame characteristics and Duration.

Membership

Administrators apply policies based on the user’s group membership within the enterprise directory; Cylentium Zero Identity supports integration with Microsoft’s Active Directory and NT Domain Server, as well as with LDAP. Integration with Active Directory and Windows Domain Server is automatic, simply by installing the Cylentium Zero Identity Directory Connector, a small application which runs on any Windows machine that is a member of the domain; integration with LDAP requires minor schema integration, dependent on the ownership LDAP architecture. This greatly simplifies ongoing management while lowering total cost of by ensuring that user moves, adds and changes within the enterprise directory automatically propagate throughout wireless access policies.

Per-frame characteristics

Cylentium Zero Identity provides for significantly enhanced security versus typical wireless security solutions by enabling filtering of all traffic to and from the Cylentium Zero Identity Client. This capability allows security and network administrators to segment and filter traffic based on user identification, network, protocol, and type of frame; these filters can be applied unidirectionally, providing for the creation of extremely granular network access policies. Policies are enforced at each WAC, even when a user roams between WACs on different subnets.

Duration

Administrators can configure session duration using two different methods—session length timeout and idle timeout. Administrators typically set session length to be slightly longer than the typical duration of the user's workday; after this pre-defined period, the user will be prompted to re-enter his/her credentials to continue as an authorized user. The session length timer considers the mobile user roaming throughout the secure wireless network, ensuring that the user cannot bypass the session length timer simply by moving from subnet to subnet. Contrast session timeout, which is used as part of all policies, with idle timeout, which some enterprises may choose to not implement. Idle timeout is typically used in those environments requiring the utmost security; examples include healthcare, financial, and government applications. Administrators can configure very short idle timeout values to ensure that a user who leaves the mobile device idle is not placing the device (or network resources) at undue risk. For instance, a healthcare worker who leaves an authorized PC/PDA connected during a lunch break may be placing the enterprise at risk of violating HIPAA security guidelines. The ability for the session to automatically time out after an administrator -defined period is a powerfully elegant mechanism to provide additional security and management without compromising the user experience.

Cylentium Zero Identity Session Model

Session Creation

Cylentium Zero Identity's authentication process is managed using an IEEE 802.1x framework and TLC-specific protocol extensions to prevent session hijacking or denial of service attacks. A unique 802.1x port is created on the WAC for each active connection. By using two-way EAP-TTLS to protect the authentication process (see figure 2), administrators are assured that the user's credentials are immune to attack and compromise. As part of the authentication process, a TLS master secret is derived, which is used in the dynamic generation of per-user, per-session AES data privacy and HMAC SHA-1 message integrity keys. FIPS 140-2 validation ensures that this process occurs according to rigorous, defined guidelines, providing administrators with mutual authentication.

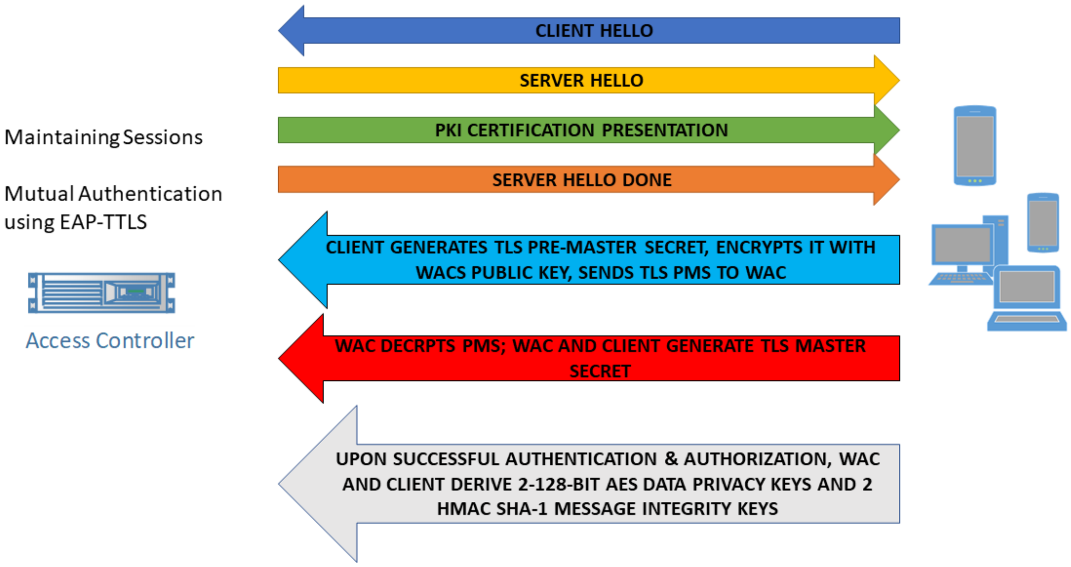
CLIENT HELLO
SERVER HELLO
PKI CERTIFICATION PRESENTATION
SERVER HELLO DONE
CLIENT GENERATES TLS PRE-MASTER SECRET, ENCRYPTS IT WITH WACS PUBLIC KEY, SENDS TLS PMS TO WAC
WAC DECRPTS PMS; WAC AND CLIENT GENERATE TLS MASTER SECRET
UPON SUCCESSFUL AUTHENTICATION & AUTHORIZATION, WAC AND CLIENT DERIVE 2-128-BIT AES DATA PRIVACY KEYS AND 2 HMAC SHA-1 MESSAGE INTEGRITY KEYS
Maintaining Sessions
Mutual Authentication using EAP-TTLS
Access Controller

Figure 2 – Sessions and 802.1x states

Maintaining Sessions

Once the secure session is established, the Client and the WAC fully authenticate each frame by validating sender identity, checking for evidence of tampering, ensuring that the frame sequence numbers are correct and verifying conformance to the policy in place for the connection.

Ending Sessions

All Cylentium Zero Identity sessions expire after an administrator-defined period, configurable per policy. Ten minutes prior to the session's scheduled expiration, the user is prompted to provide authentication credentials so the session can continue without interruption. If the user is not available to provide credentials, the session expires on all WACs simultaneously, and all session keys are erased.

Mobilizing Sessions

Cylentium Zero Identity supports three types of secure mobility. The basic mechanism for re-establishing a connection between the Client and a new WAC is the same for all three mobility modes. Upon the successful creation of a new session, the Manager downloads the security context to all available WACs. This information is used to facilitate low-latency handoffs as users roam between WACs. When the Client roams from one Cylentium Zero Identity-secured subnet to another and establishes a new radio connection, the new WAC uses the Client's session context (pushed to each WAC when the user originally established the session) to complete an abbreviated TLS handshake. In doing so, the Client is securely authenticated on the new Cylentium Zero Identity-secured subnet. No intervention is required on the user's part, making roaming a seamless, transparent process for the user. Each time a user roams between secure subnets, the roam is logged to ensure accounting and ease troubleshooting for the administrator. As noted, Cylentium Zero Identity provides three options for robust mobility support—the option for a user to maintain an IP address as he/she roams between subnets, ensuring application integrity; the option for a user to always attach to a given subnet, appropriate for those enterprises using static IP addresses; and the option for a user to receive a new IP address each time he/she roams between subnets. The first option is the option used in most cases.

Encryption

The Advanced Encryption Standard (AES)

Cylentium Zero Identity utilizes AES to protect sessions and networks from attack and compromise. AES is a Federal Information Processing Standard (FIPS) which specifies a cryptographic algorithm for use by U.S. government organizations to protect sensitive information. AES' combination of security, performance, efficiency, ease of implementation and flexibility make it an appropriate selection for mobile applications using Cylentium Zero Identity. AES is ideal for lightweight hardware devices such as PDAs, ensuring maximum battery life and throughput by minimizing processing needed to execute encrypted sessions. Contrast AES with Triple DES, which can suffer overhead of 30% or more; further, the processor-intensive nature of Triple DES will drain battery life at a much greater rate than will AES.

Due to its performance characteristics, AES is specified as the data privacy algorithm in the 802.11i security standard. However, since existing 802.11a/b/g/j/n network interface cards and access points employ encryption mechanisms (WEP, Dynamic WEP, WPA) using hardware-based RC4, the vast majority of existing access points will need to be replaced (either in whole or in part via a firmware and/or radio card upgrade) to support 802.11i. Cylentium Zero Identity offers all the benefits of AES-based data encryption today , while adding significant enterprise-level management and mobility features which are not addressed by the standards bodies. Further, Cylentium Zero Identity protects the existing investment in access points and network interface cards by eliminating the need for a "forklift" upgrade to move to 802.11i; standards-based products can be used in a "mix and match" environment, further increasing return on investment while lowering total cost of ownership.

Future Standards Architecture Today

Cylentium Zero Identity deviates from 802.11-2007 in some respects to overcome deficiencies that are not addressed by the IETF Working Groups:

1. 802.11 calls for Security identification and negotiation in 802.11 *management frames*. Cylentium Zero Identity is compliant with the RSNA (AES-CCMP, 1x), but does not use management frames because:

Supporting this requirement literally would require the ability to control / override firmware logic in existing Access Points. This is vendor specific. The lack of a vendor neutral way of configuring and provisioning access points is a well-known **deficiency** in the 802.11 standard. IETF developed a standard called the Control And Provisioning of Wireless Access Points (**CAPWAP**) that was intended to rectify this deficiency but many Access Points still use the management frame model.

Cylentium Zero Identity supports standards-compliant key negotiation, encryption and authentication, but only after the Discovery Phase of 802.11 protocols and after association. This provisioning approach does not compromise security in any way and allows Cylentium Zero Identity to provide RSN (WPA2-Enterprise class) security even to APs that do not support it. In fact, it does not require the AP to be pre-provisioned for security at all.

2. 802.11-2007 calls for key material and 1x authenticator support on the AP. Cylentium Zero Identity does not do this because:

This is a **known weakness** in the standard because it offers no security between the AP and the Data Center, only between the user and AP. In CAPWAP terminology, this is a **Local AP**. The AP is often connected to the Data Center via long haul wireless bridge, or wire. The Local AP secures the perimeter but leaves the AP vulnerable to wiretap or physical penetration (i.e., the AP can be stolen, hacked and spoofed).

The **CAPWAP Taxonomy** extends the security boundary by also allowing a **Split AP** architecture such that the data plane between the AP and AC to be encrypted for end-to-end protection. Although the security improvements of Split AP are a huge improvement over a local AP model, the Split AP architecture has not been widely adopted. Zero Identity, unlike a standard Split AP architecture extends the security boundary to each endpoint, providing complete end-to-end security protection.

3. Cylentium Zero Identity does not publish the security method in the beacon or probe response. Again, this is primarily because it must operate after Discovery to a) support legacy devices and b) retain vendor neutrality. The secondary reason is to provide *obfuscation* of to **cloak** the security method, which leave conventional APs vulnerable to future attacks.

Cylentium Zero Identity has chosen to implement the most secure taxonomies defined by the standards, delivering the most secure solution for your home or enterprise.

Conclusion

Wireless LANs are a dynamic, unique and popular technology. IT professionals who grasp the tenets of holistic security design will understand that common wireless LAN security solutions which treat the wireless LAN as a hostile entity are not enough for truly secure enterprise-wide deployment. IT professionals will also understand that a well-designed solution for securing, mobilizing and managing wireless LANs should integrate seamlessly into existing enterprise network design and network management principles.

Cylentium Zero Identity is a unique solution to treat security, mobility and management with equal importance without compromising any of the three:

1. Security – Cylentium Zero Identity operates at Layer 2 of the OSI stack, providing the utmost level of protection against attacks end-to-end, protecting the crucial distance between the APs and data centers that conventional networks expose.

2. Mobility – Cylentium Zero Identity supports a highly mobile, vastly scalable enterprise user community with simple, elegant, secure roaming that provides a seamless user mobility experience while making the IT administrator's job easier.

3. Management – Cylentium Zero Identity enables administrators to utilize existing enterprise directories to manage and secure wireless LAN connections, regardless of the access infrastructure protocol or vendor.

Cylentium Zero Identity implements the most secure forms_of 802.11, and in the spirit of the IETF CAPWAP Taxonomy, which permits key material and configuration currently done at the AP to be done at either the AP or the AC (Access Controller). Besides more flexible provisioning and security management in the AC, the CAPWAP architecture improves security by allowing the data plane between the AP and AC to be encrypted for end-to-end security. This is precisely what Cylentium Zero Identity accomplishes today.

Govt & Military Certifications

Defense Information Systems Agency (DISA); Department of Defense (DoD); Department of Energy (DOE); Department of Defense (DnD); Department of National Defense Canada (DND)

Software Certifications

Microsoft, Linux, Apple, Symantec, McAfee

Hardware Certifications

DELL, HP, Apple, Cisco, Aruba, Checkpoint, Extreme, Palo Alto

About Cylentium, Inc.

Cylentium and Zero Identity secures enterprise wireless local area networks by providing Cylentium Zero Identity, the industry's only FIPS 140-2 certified Layer 2 software security solution. Cylentium Zero Identity encrypts full Ethernet frames, rather than just IP payloads, hiding vital information such as IP addresses, applications and ports from unauthorized listeners. Frame-level encryption also protects non-data network traffic, including DHCP requests or ARP messages, which can be compromised and used to attack the network. This approach helps protects both the user's data and the organization's network, while enabling users to securely roam across subnets without needing to re-authenticate or reboot, saving time and minimizing frustration.