Authentic Web

ENTERPRISE DOMAIN MANAGEMENT FOR THE NEW TLD ERA

4 USE CASES

A NEW NETWORK SECURITY SERVICE

Extending the Trust Anchor of a Brand Top Level Domain

*Protect your company data
and keep customers safe.*

4 **DIGITAL NETWORK USE CASES** demonstrate a new security model anchored on the CONTROL and TRUST authority of a Brand Top Level Domain. Business stakeholders and IT security management can protect customers, partners and enterprise data-in-motion at scale. Trust authority attributes of the Brand Registry, under a new management system make it easy to establish security automation, monitoring and remediation in a safe, TRUSTED brand space.

USE CASE AUDIENCES

BUSINESS LEADERS

Consumer Brand Trust is Essential to Business Success.

✓ *Responsible for the enterprise brand growth and success*
✓ *Mandated to protect and maximizing brand trust*
✓ *Mission to deliver a differentiating brand strategy*

BUSINESS GROWTH

BRAND TRUST

BRAND DIFFERENTIATION

IT AND NETWORK INFRASTRUCTURE LEADERS

Securing data is getting harder, more costly and increasingly important.

✓ *Mandated to improve IT security under increased external threats*
✓ *Exposed to compliance gaps under more rigorous regulatory regimes*
✓ *Motivated to find scale and efficiency with budget and headcount limits*

SECURITY THREATS

REGULATORY COMPLIANCE

OPERATIONAL EFFICIENCY

Protect your company data and keep your customers safe.

REGISTRY TRUST MANAGER™
- AT A GLANCE

The Registry Trust Manager (RTM) from Authentic Web Inc, is an end-to-end security service that encrypts and authenticates data-in-motion over a wide variety of network connections. Anchored on the superior trust authority of a Brand Top-Level Domain, it empowers teams to gain network security visibility, and control while reducing compliance and administrative effort and cost.

RTM IS A BRAND REGISTRY-BASED SECURITY & COMPLIANCE TRUST SERVICE

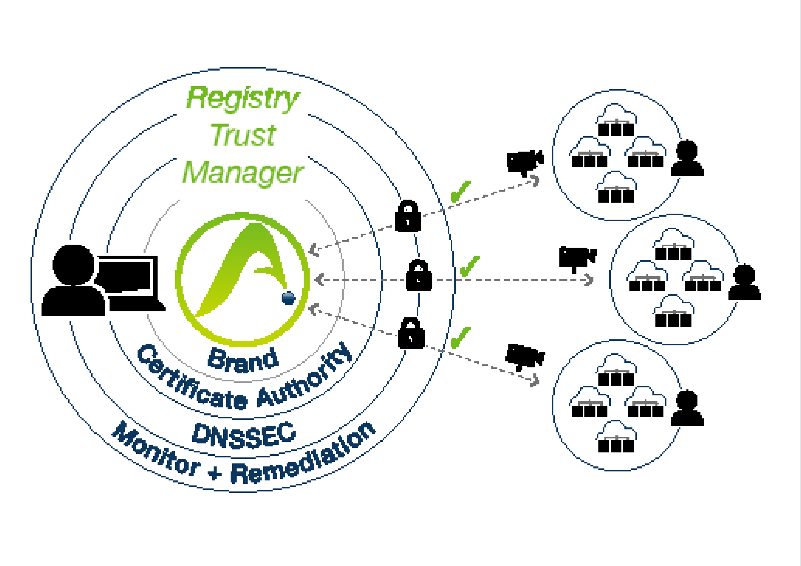
All connections are authenticated on a proprietary Brand Top-Level Domain (TLD)

- ✓ *TLS certificates are enforced and monitored*
- ✓ *All data in transit is route-protected with DNS security extensions (DNSSEC)*
- ✓ *All connections are monitored for TLS and DNS security policy compliance*
- ✓ *Fully automated workflow reduces cost and scales easily*
- ✓ *Change management auditing and digests alert team members to changes*
- ✓ *Monitoring and remediation prevent data transit over unsecure connections*
- ✓ *TLS version control, with cipher suite visibility at all endpoints*

USE CASES

Supply Chain, Internal and External Applications, IoT, EDI, WIFI or any server-server or server-client data network requiring assurance of data-in-motion encryption, route assurance and identity access authentication.

An end-to-end automation toolset to efficiently protect company and customer data at scale.



RTM anchors on the TRUST authority of a Brand Top-Level Domain with client-specified security policies including DNSSEC and TLS certificates to all endpoints. In addition, the unified, automated control environment monitors all specified network endpoints to ensure compliance with enterprise data network security policies. A number of known security vulnerabilities with DNS and TLS are eliminated. Network management teams benefit from improved transparency, control, remediation and an ability to scale with significantly reduced effort and PKI lifecycle management risk.

WHAT IS THE PROBLEM?

Attacks and data breaches have increased tremendously over the last decade. As the chart below illustrates, data breaches have risen by a factor of six, from fewer than 200 in 2005 to more than 1,300 in 2017 -- a worrisome trend that continues into 2019.

While organizations have embraced and adopted stronger security practices, reliance on old and outdated manual processes such as **password management** stubbornly persist.

For **device authentication**, although PKI is superior to pre-shared keys, the complexities of key management and certificate revocation lists expose organizations to administrative errors and security risks. When client certificates expire, new certificates must be generated and signed by internal/external CAs and installed on client endpoints. The complexity and work effort in these process tasks impede adoption of PKI on end device certificates, leaving them exposed.

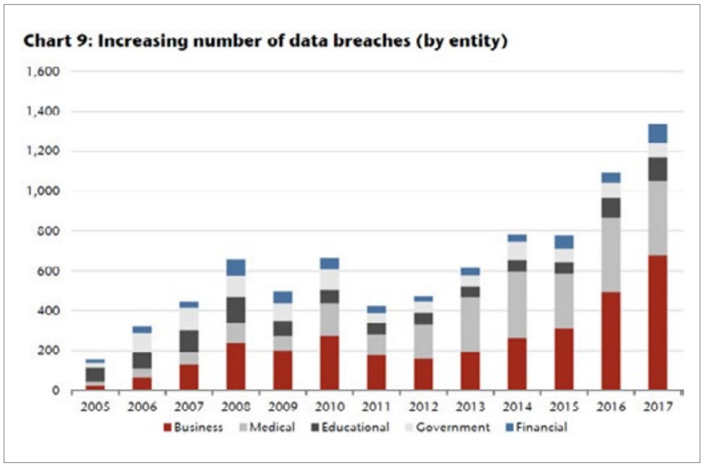


Chart 9: Increasing number of data breaches (by entity)

Source: Markewatch.com

The Registry Trust Manager (**RTM**) is a fast, secure, system-based approach to data network encryption and authentication that eliminates manual work effort. It scales easily to thousands of endpoints, removing the human factor errors known to place network security at risk.

RTM USE CASE 1
SECURE MOBILE IOT

SERVER MODEL

Older IoT architectures ran a webserver that allowed clients to connect to devices with a User ID and password combination. We all are familiar with printers and WIFI routers accessible over plain HTTP.

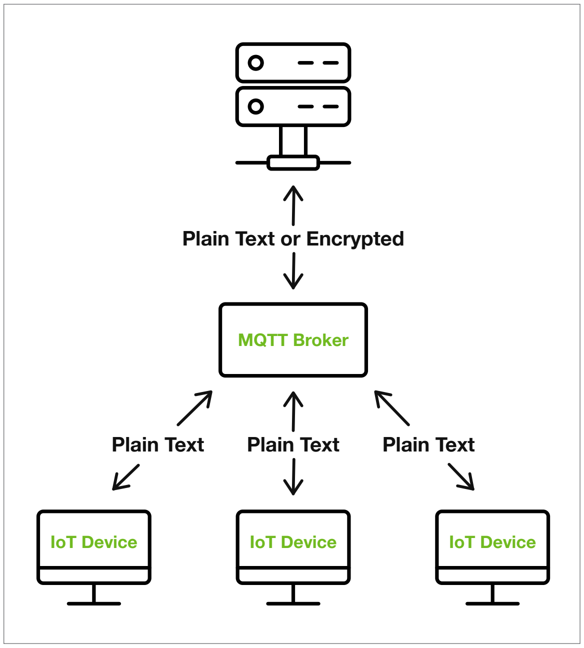
Newer architecture IoT devices hold a long-lasting connection to an MQTT broker that might send commands, receive data, and route messages. These new devices have memory and CPU to adequately handle the demands of PKI. As such, communicating with an MQTT broker over TLS is gaining traction. Nonetheless, challenges around issuance, chain of trust and certificate lifecycle management remain a problem, particularly at scale, making the practice impractical, until now.

Using RTM, device manufacturers (DMs) and their customers no longer need to trade off security for added complexity and cost factors. RTM allows a DM or its customers to effortlessly deploy certificates and monitor and manage all endpoints with the trust anchor of a Brand Top-Level Domain.

CLIENT MODEL

In a Client model, devices simply connect to external systems and typically subscribe to or publish information. A PKI can greatly enhance the security of this model. Client certificates can be introduced to authenticate the client with the server. Using RTM as your PKI lifecycle management system in the Brand TLD space, addresses network trust, ease of management for teams and scalability.

This diagram shows a simple IoT architecture and the non-encrypted communication stream between IoT devices, MQTT Broker and servers. The data in transit may or may not be encrypted with certificates. If they are HTTPS equipped, teams struggle to ensure certificate renewals are processed properly at scale.



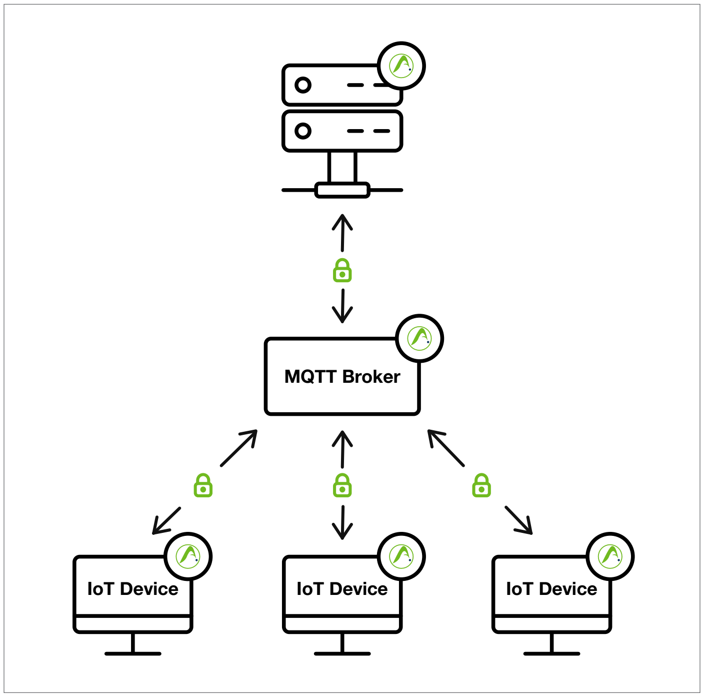
PKI infrastructure is difficult to manage and implement for IoT devices. If a DM or its customer issues self-signed certificates for a device, the IT team must manage the expiration and renewal of the certificates on a perpetual basis, with zero-errors. While long expiration dates can mitigate the administrative workload, the renewal and installation effort and required attention to detail remains. Importantly, shorter term certificates are recommended as a security best practice since certificates with weaker encryption algorithms can be swapped out in shorter intervals.

Using RTM, an IoT architecture can quickly plug in a PKI infrastructure, anchored on the trust authority of the Brand TLD to extend trust with a system-enforced HTTPS policy.

RTM EQUIPPED IOT NETWORK

This diagram shows how RTM can protect the communication stream between all devices and the MQTT Broker through to the servers, pushing and pulling data from the IoT device network.

The RTM Agent automates certificate provisioning and rollovers with the integrated, trusted CA. RTM automates the issuance, monitoring, expiring and revocation of all certificates thereby automating the lifecycle in a PKI infrastructure. Additionally, remediation in a single control environment eliminates typical chain of trust vulnerabilities common to siloed systems and human-dependent, manual processes.



The RTM architecture can segment IoT networks into Clients and Client Groups to set policies according to specific business requirements (of a use case) in a configurable hierarchy. Teams can view, manage and set remediation policies accordingly and scale it to secure the entire IoT network.

RTM USE CASE 2
EXTENDED ENTERPRISE APIs

In architectures where Enterprise A offers an API and Enterprise B communicates with this API there are often strict identity and access requirements including IP restrictions and Application Keys to identify an application.

APPLICATION USE CASES

Supply Chain, Logistics, and EDI - Multiple supplier entities may communicate inventory levels or pricing information to distributors.

Information and Transactional Brokers – Common to supply chain or other financial services use cases.

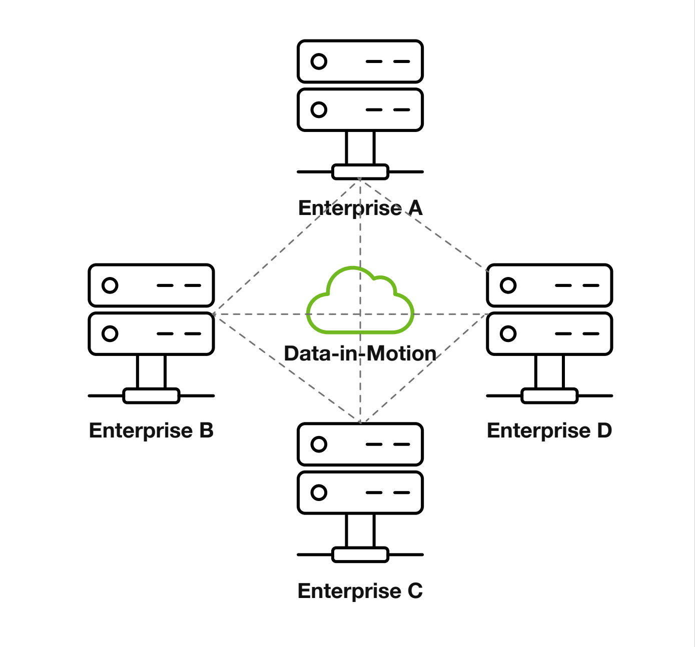
Medical institutions/Health Care - Required to share patient (Electronic Medical Records) EMR with a central authority.

Other applications include networks and/or middleware providers that broker data exchanges and transactions between parties and/or where enterprise network architectures extend to the cloud.

Deploying RTM as a PKI management tool seamlessly and efficiently secures data-in-motion and ensures identity access in a trusted brand space when connecting endpoints between parties. RTM allows an organization to centrally manage the full certificate lifecycle including:

- *Certificate issuance and deployment (including client certificates) on endpoints*
- *Revocation of client certificates, and/or installing new certificates.*

RTM also adds route authenticity by automating DNSSEC provisioning and key rollovers

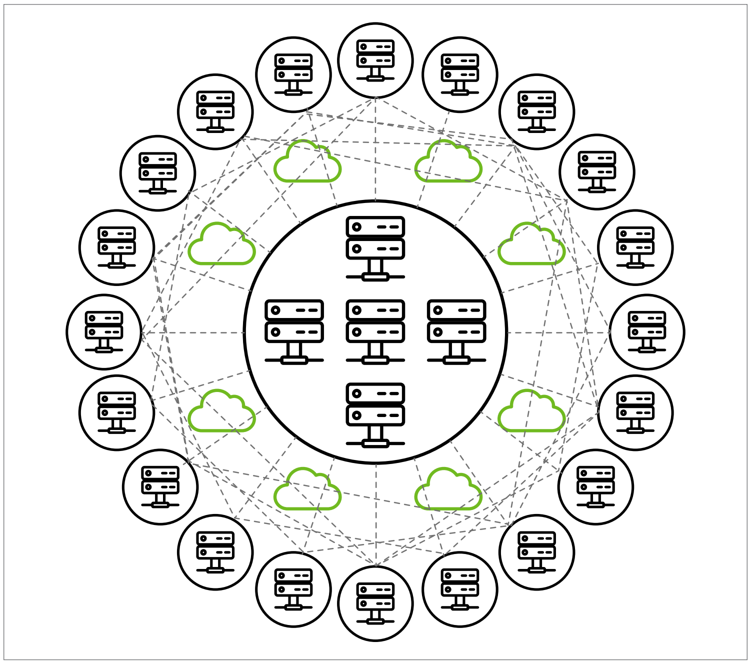


Centralized management and reporting empower infrastructure teams with full visibility over the status of all endpoints, any non-client exceptions, and/or revoked certificates. The tools allow monitoring of third-party vendor compliance, for issues such as outdated SSL/TLS cipher suite versions installed on third party endpoints. (Old TLS versions have known encryption vulnerabilities that place data-in-transit security at risk.)

In the figure below, consider the work effort to enable and maintain just 20 third party endpoints using PKI. RTM reduces laborious, manual process tasks, including:

- *Creation, installation and management of certificates lifecycles including renewals and verification*
- *Establishing DNSSEC at the registry and DNS and managing annual DSKEY rollovers*
- *Establishing monitoring systems to policies and manually remediating broken connections.*

RTM eliminates the errors and omissions of personnel who forget, don't bother or make mistakes.



The work effort case for 20 endpoints is daunting. On operating scales of 100s or 1,000s of endpoints, fully compliant security operations become unfeasible in the absence of an automated system and protocol to provision, monitor and manage the lifecycle of mission critical network connections.

RTM offers a key differentiating opportunity for organization to ensure trust, since it's anchored on the Brand Top Level Domain. All connections terminate or originate in the trusted namespace that is fully controlled and owned by the brand. This is a key concept to extend the validation of trust. Enterprise vendors and partners that establish trusted network connections to an RTM-protected enterprise, are assured that all endpoints are secured and managed in line with Zero Trust to protect company and customer data.

RTM USE CASE 3:
WIFI DEPLOYMENTS (EAP-TLS)

Credential theft is a serious issue in corporate environments. With over-the-air attacks occuring more frequently, organizations have turned to WPA2 and EAP-TLS to help secure their networks. A client certificate is used to authenticate the client to the network, while a server certificate validates the network to the client. Both the client and the network will verify the authenticity of the respective trusted certificates.

EASY ONBOARDING

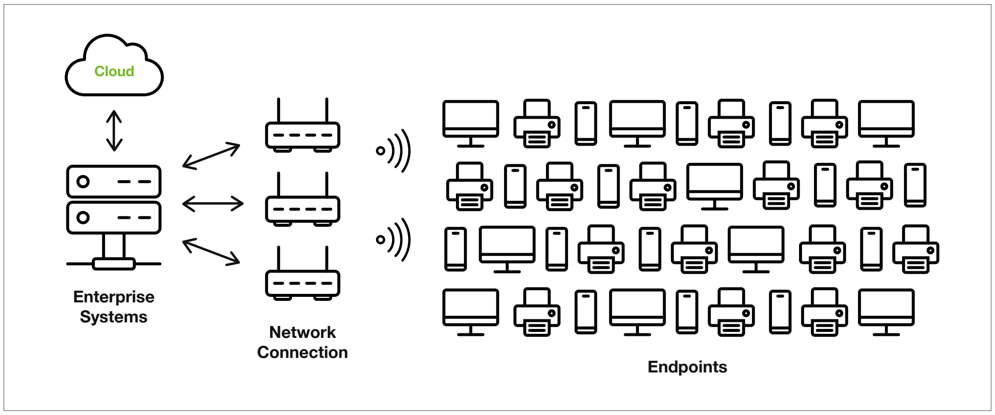
RTM clients simplify the onboarding/authentication of a new device on the network by streamlining the process of downloading the correct certificates for end user devices. Policies set within RTM can govern the expiration of user certificates, which in effect, forces a password change policy without using passwords.

NO PASSWORDS

RTM eliminates user passwords and the assocated administrative effort to manage them. Certificates can be set to expire quarterly minimizing the window of opportunity for an attacker. Users and IT staff alike experience reduced frustration and work effort.

POLICY CONTROLS

RTM lets IT staff and administrators set policies to automatically revoke a certificate once a user is terminated. User authentication management can be integrated with Active Directory. Administrators may still revoke certificates manually, should they wish. Users can be grouped by department for configurable certificate policies by group.



GENERIC USE CASES: *CERTIFICATE-BASED AUTHENTICATION*

We know that accessing systems with legacy User ID and passwords is a poor security practice, yet it's common, largely due to the lack of a better solution. RTM can establish authentication without the need for passwords and associated, and insecure password management overhead.

IDENTITY AND ACCESS MANAGEMENT

Zero Trust is based on criteria authorizing access: 1. Who is connecting, 2. Why are they connecting, 3. What is the user context of connecting. RTM offers established x.509 authentication capabilities for internal and external applications vs. relying on manually configured authentication rules that are inconsistent across the enterprise.

WEAK PASSWORDS

Human nature is to re-use the same password (if corporate systems allow it), choose extremely simple passwords, and/or keep password reminders around the work area. A recent study by the UK's National Cyber Security Center noted that over 23 million people used '123456' as their password. RTM authenticates users more securely without the use of easily misused passwords.

SPEAR-PHISHING

Employees are vulnerable to socially engineered email (BEC) that can compromise their user credentials. Despite anti-phishing measures in most organizations, compromised access credentials remain the principal tactic for hackers to access corporate networks and systems. RTM eliminates the use of passwords that are vulnerable to phishing.

EASE OF USE

Certificate-based authentication is much simpler and easier to manage than password authentication systems and manual certificate lifecycle administration. RTM helps reduce IT support staff effort, freeing up valuable resources.

The Registry Trust Manager is a robust identity and access security framework that significantly reduces the risk of a data breach due to stolen security credentials or poor staff password management.

USE CASES SUMMARY

These first use cases provide enterprise infrastructure teams with several examples where the Registry Trust Manager can secure Server to Server, Server to Client and IoT endpoints on internal and external networks and applications. Once deployed there are various opportunities to extend the RTM enabled trust network to peripheral endpoint and data protection technologies. RTM capabilities allow network engineers to first anchor the network in a trusted state from which to build new layers of protection.

ENTERPRISE TRUST AND OPERATIONAL EFFICIENCY VALUE

Today, infrastructure teams rely on personnel diligence and manpower to implement authentication and data-in-motion security policies. Business leaders may trust their team's intent but cannot guarantee that every managed connection is locked down without fail, every time, without exception. Staff moves and departures create further risk of dropped oversight during hand-offs. The RTM solution maintains the integrity and knowledge base to view and manage all enabled secure connections.

The Registry Trust Manager extends the trusted Brand TLD space to guarantee connection security. Authentication and encryption are fully established in a single control environment to enforce connection lifecycle compliance. Automation, simplicity and ease-of-effort in managing complex security policies at scale offer a new capability to infrastructure teams.

- *Automated provisioning and management of data network security policies*
- *Economically scalable to an unlimited number of endpoints*
- *Establishes an authoritative, trusted network that is secure and monitored*
- *Low work-effort to establish and maintain extensive endpoint deployments*
- *Brand **TRUST** in network operations. Internal and External.*

USE CASES

SUPPLY CHAIN

CLOUD

IOT

APPLICATIONS

EDI

RTM is a network security innovation based on the ability of brands to own their Brand Top-level Domain where full control and enforced policies extend TRUST.

The model can be applied to use cases or to the entire enterprise network as the anchor of TRUST to protect company, partner, supplier and customer data.

WANT TO KNOW MORE? CONTACT US

Automation to improve data SECURITY and COMPLIANCE
anchored on the TRUST authority of your BRAND REGISTRY

AUTHENTICWEB.COM
info@authenticweb.com
NA 1.855.436.8853 | International +1.416.583.3770