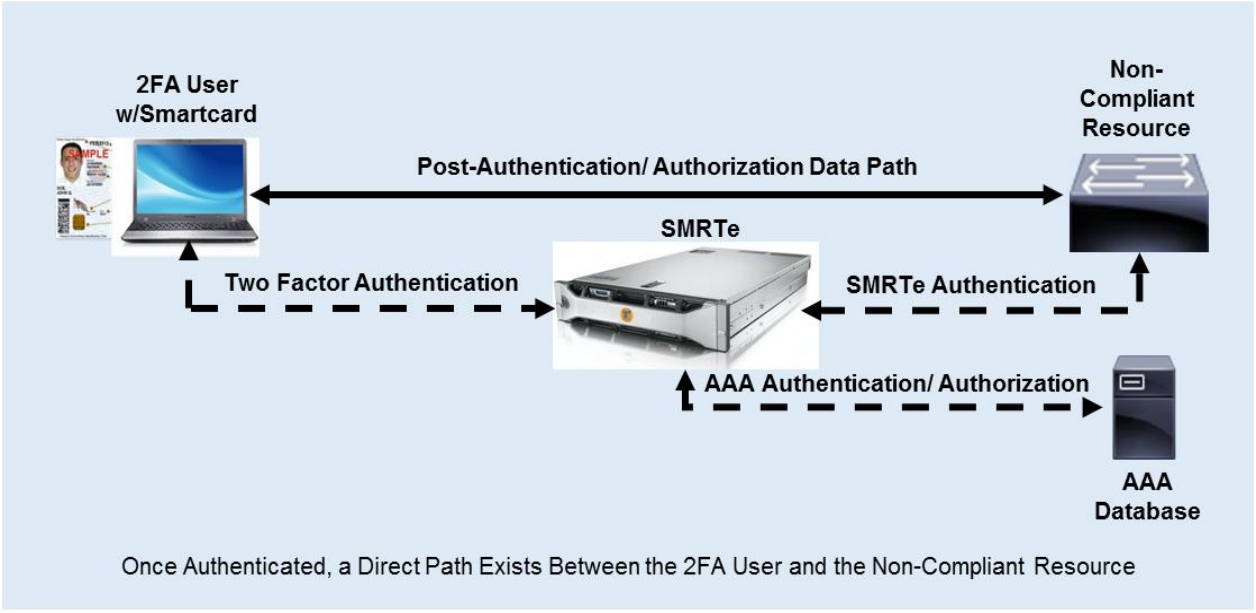
SMRTe – Enabling Network-Wide Two-Factor Authentication

SMRTe Allows Users With Secure Two-Factor Authentication (2FA) to Directly Access Network Resources That Employ Only Unsecure Username and Password Authentication.

In today's Cybersecurity atmosphere more and more network planners are adopting Two-Factor Authentication (2FA) methods to ensure secure access into their networks. While many organizations are now using 2FA to manage access into their network from the outside, few utilize it to manage access to network resources (i.e., devices and applications) by users who are already inside the network. This situation, known as: "Hard on the Outside/ Soft on the Inside" creates a breeding ground for all types of unwelcomed "Insider Threat" scenarios. Since upgrading these, so called: "non-compliant" resources to 2FA is a very costly proposition, network planners have configured a way of essentially "hiding" them behind firewalls or reverse web proxies and, in effect, extending the VPN concept inside the network. This solution requires a major network re-design and can result in reduced performance by adding latency and potential bottlenecks.

The SMRTe presents a straight-forward and "elegant" solution by implementing network-wide secure 2FA for all network resources thus making the network "Hard on the Outside AND Hard on the Inside." The **SMRTe** eliminates the use of passwords by network resources therefore eliminating the need for firewalls, VLANs, or subnets. This reduces upfront network re-configuration costs and the need for purchasing additional security tools. The **SMRTe** has minimal impact on network performance including latency, bottlenecks and management headaches.



Once Authenticated, a Direct Path Exists Between the 2FA User and the Non-Compliant Resource

SMRTe Benefits

No Firewalls - Using the **SMRTe** eliminates the need for firewalls in the network. The patent-pending technology employed by the SMRTe ensures that hackers cannot perform a brute force password attack.

No Passwords - The **SMRTe** is the only solution that does not rely on passwords anywhere in the authentication process. While other Single Sign-On (SSO) solutions claim to get rid of passwords still rely on passwords to log into underlying network resources. These passwords are hidden by firewalls or reverse web proxies to prevent brute force attacks or hackers accessing the password database. A major concern with this approach is that if the solution fails the network resource is locked out. This is a particular concern with Privileged Access Management solutions.

2FA Flexibility - The **SMRTe** supports several popular 2FA methods such as Smartcard, US Government issued Common Access Card (CAC), RSA SecureID, hard tokens, biometrics, etc. Furthermore, if at any time a new 2FA method gains popularity, a new software app can be generated and loaded into existing SMRTe units to accommodate users of this new method of authentication. No changes will be required to existing network resources.

No Generic Login - The **SMRTe** promotes a positive security approach and best business practices in the organization since it does not allow users to login using generic usernames like “administrator” or “user”. This promotes user-specific auditing for network resources which is crucial for auditing as part of threat mitigation.

AAA Flexibility - User authentication and authorization is accomplished through a variety of centralized Authentication, Authorization and Accounting (AAA) servers. The **SMRTe** can be integrated with any existing AAA servers including RADIUS, TACACS+, LDAP, and Active Directory.

SMRTe Security

The **SMRTe** can be deployed as a hardware appliance, a software application, or a virtual appliance. It requires no changes to user devices, network devices, applications, or network architecture. As such it is an ideal addition to existing networks as well as new networks.

The **SMRTe** is the enterprise version of the SMRT currently deployed by the Defense Information Systems Agency (DISA). It was designed in compliance with Department of Defense Public Key Infrastructure and Security and Technical Implementation Guides (STIGs).

The **SMRTe** uses only FIPS 140-2 validated algorithms and modules for any and all cryptographic functions.

The **SMRTe** enforces Security-Enhanced Linux (SELinux), a Linux kernel security module that provides a mechanism for supporting access control security policies, including DoD–style Mandatory Access Control

TELEGRID Technologies Inc.
23 Vreeland Road
Florham Park, NJ 07039

973-994-4440
sales@telegrid.com
www.telegrid.com

TELEGRID