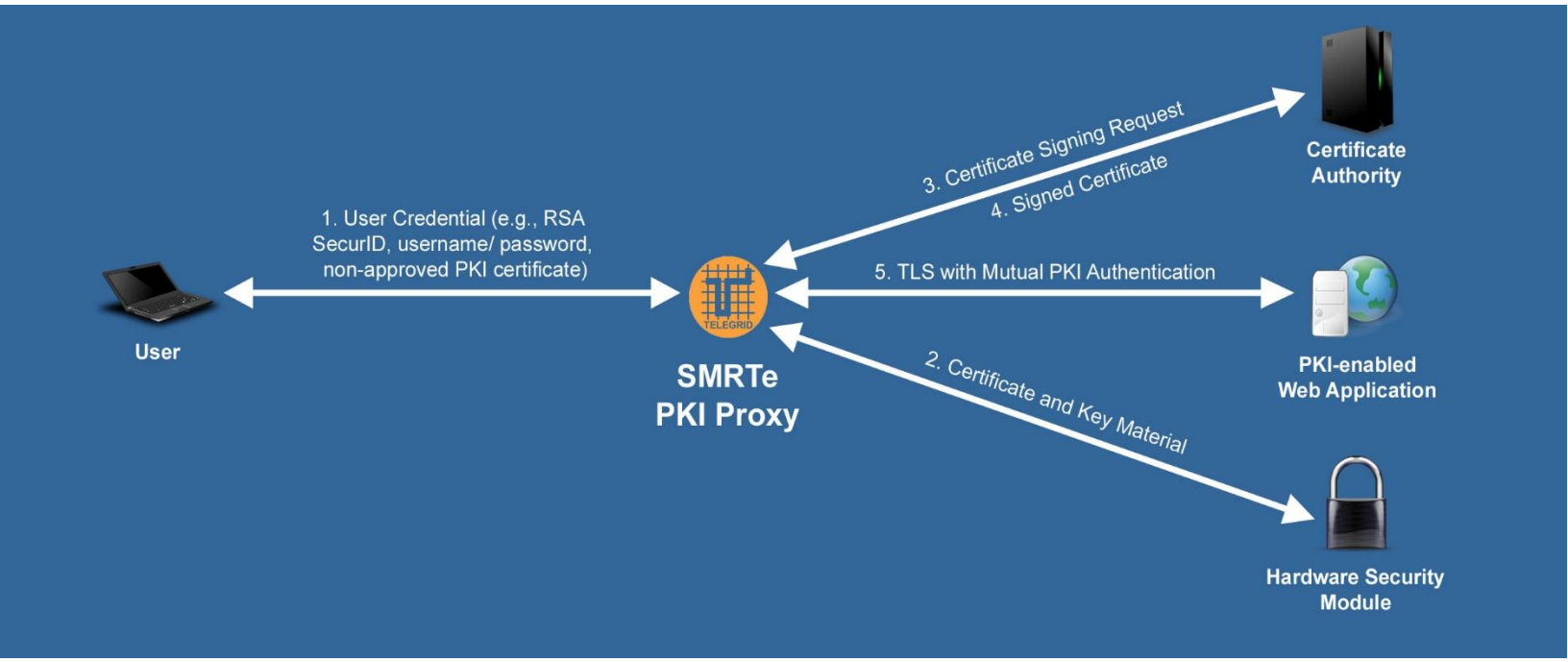
SMRTe PKI Proxy

P/N: RWP-1801

TELEGRID

TELEGRID's SMRTe PKI Proxy dynamically generates user-specific PKI certificates in order to allow seamless implementation of PKI within existing Identity Management infrastructures. The PKI Proxy:

- Resolves authentication token cybersecurity issues
- Operates with any Single Sign-On infrastructure
- Converts any authentication credential type to a Public Key Infrastructure (PKI) certificate
- Promotes network-wide TLS with mutual authentication
- Allows cross-domain PKI with root of trust
- Allows short term PKI certificates to simplify revocation checking
- Promotes NIST 800-63-3 Holder of Key compliance



PKI is the most secure method of providing Multi-Factor Authentication (MFA) and information flow in modern networks. PKI certificates combine an individual's identity information with cryptographic information that is non-forgeable and non-changeable. They provide a standards-based representation of the individual's physical identity in electronic form and enable data sharing among appropriate, broad and dynamic communities of interest.

TELEGRID Technologies, Inc.
973-994-4440
sales@telegrid.com
www.telegrid.com

TELEGRID

SMRTe PKI Proxy

P/N: RWP-1801

TELEGRID

PKI with Mutual Authentication

PKI with mutual authentication ensures the integrity and confidentiality of devices and resources operating on a network. It also enables management of identities operating in groups or certain roles within systems. Due to the issue of managing user PKI certificates many organizations only implement server side certificates for secure TLS communications. The SMRTe PKI Proxy accepts any user credential type and automatically generates a unique PKI certificate that can be used for mutual authentication and authorization.

Short Term PKI Certificates

One of the major issues with the management of PKI certificates is revocation or removing the rights of individuals who have left an organization. The reason is that the validity period of PKI certificates is normally two years so revocation lists must be updated and disseminated quickly. The SMRTe PKI Proxy resolves this issue by allowing the dynamic generation of short term certificates drastically reducing the revocation attack vector.

NIST 800-63-3, Holder of Key and Break and Inspect

In June 2017, NIST released the NIST 800-63-3 Digital Identity Guidelines which cover all aspects of user authentication from initial risk assessment to deployment of federated identity solutions. For the most secure systems, those that are deemed FAL3 for Federated Assurance Level, the NIST guidelines require that a user present a proof of key ownership in addition to an authentication token. This is referred to as Holder of Key and is a requirement of the Federal Government, the military, and most government contractors. This was instituted because relying solely on authentication tokens exposes the network to several cybersecurity attacks.

Authentication Token Cybersecurity Attacks

- Man-in-the-Middle
- Compromised Tokens
- Denial of Service
- Assertion Repudiation
- User Re-authentication

Holder of Key creates an issue for most networks since, according to the SAML and OAuth standards, the only approved method for implementing Holder of Key is through PKI and TLS with mutual authentication. Most networks break TLS connections, a process known as “Break and Inspect”, in order to examine message contents. This makes passing user PKI certificates and Holder of Key impossible. The SMRTe PKI Proxy is the ONLY product that dynamically generates PKI certificates to satisfy Holder of Key.

SMRTe Features

- FIPS 140-2 Level 1 Compliant Encryption Engine
  - Symmetric Key CryptographY
  - Public / Private Key Pair Generation
  - Hashing
  - Random Number Generation
- Public Key Infrastructure
  - Certificate Revocation Checking (OCSP and CRL)
  - X.509v3 Standard Certificates
- DISA Security and Technical Implementation Guide (STIG) compliant
- Security Enhanced Linux (SELinux)
- Available as a Virtual Machine or as a Hardware Appliance

TELEGRID Technologies, Inc.
973-994-4440
sales@telegrid.com
www.telegrid.com

TELEGRID