SKI™
SECURE KEY INFRASTRUCTURE

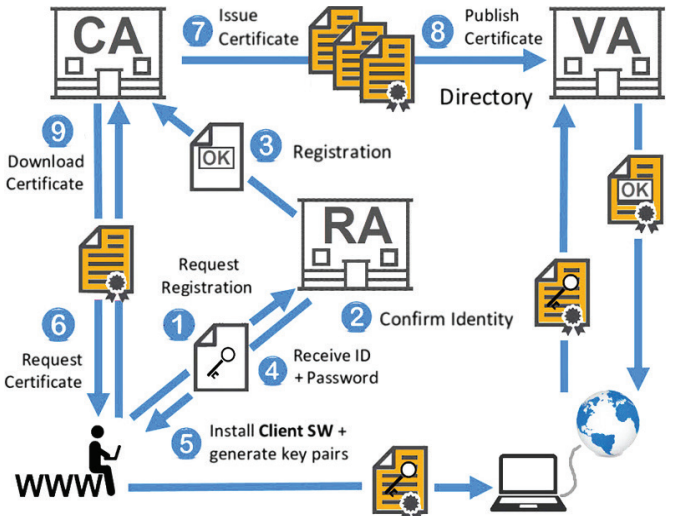
SECURE KEY INFRASTRUCTURE

The simple, secure alternative to certificate-based PKI

THE PUBLIC KEY INFRASTRUCTURE (PKI) IS COMPLEX, CUMBERSOME AND CAN BE COMPROMISED

ISSUES	RISKS
Too Many Moving Parts	Eavesdropping
Doesn't Scale Well	Signed Malware
Unusable for IoT	Compromised CA/RA
Bad Trust Actors	Non-Repudiation
Quantum threat to asymmetric encryption	Man-in-the-Middle
	Expired Certificates

PUBLIC KEY INFRASTRUCTURE



THE ALTERNATIVE - SECURE KEY INFRASTRUCTURE (SKI)

Secure Channels' patented Secure Key Infrastructure (SKI) process utilizes an existing network of global cloud services for speed, reliability, and uptime for efficient encryption key distribution.

The SKI process utilizes OAuth 2, HTTPS and TLS 1.3 to secure communications between clients and servers during the key exchange process.

The SKI process is extremely efficient in using a Token Authority(TA), non-identifying tokens, and a double-blind randomization process that confirms only the intended recipient will receive the encrypted data and be able to decrypt it. All users register their ID and devices during the sign-up process.

The SKI process is extremely extensible and has proven to be equally effective in providing efficient and secure key distribution using any combination of satellites, drones, vehicles, devices, wearables, processors, etc., in both internet-connected and non-internet-connected environments.

SECURE KEY INFRASTRUCTURE (SKI)

THE BENEFITS ARE CLEAR

- Leverages existing cloud services networks
- Can be implemented using a combination of public/private/cloud services & edge networks
- Fault tolerant
- Highly available
- Highly scalable
- Mitigates against DoS attacks
- Mitigates against DDoS attacks
- Mitigates against MITM attacks

THE PROCESS

- Sender requests a token from token authority (TA). TA responds and issues token. (The token is non-identifying and only pertains to the data to encrypt)
- Data encryption begins and symmetric encryption keys are sharded into key segments.
- Key segments and token are sent to cloud network. (Double-blind randomization process takes place)
- Cloud services network sends token to TA for verification. TA generates new toke and sends it to cloud network.
- Recipient connects with TA to receive new token and connects with cloud services network to receive key segments
- Recipient is now able to successfully decrypt data.