Solution Brief

Pulse Secure

Pulse Secure and CASQUE SNR Identity Assurance

Military Strength Security for Pulse Connect Secure SSL VPN

- ✓ Scalable Authentication System
- ✓ Prevents Token Cloning
- ✓ Resists Insider Attacks

Authentication techniques based on fixed targets can be compromized and remain undetected

Security compromizes through malware, phishing exploits or even privileged insiders are difficult to detect and prevent, and can easily damage a company's reputation.

CASQUE SNR's keys are changed dynamically and invisibly, removing fixed targets and so are immune to insider attacks, token clones and manufacturer reveal.

Pulse Secure

+

CASQUE SNR

Challenges

Not All Authentication Techniques Are Strong

Methods using biometrics, knowledge or one-time-password dongles based on fixed keys are all useless when exposed by an insider or penetration attack.

Avoid Systems Built on Insecure Infrastructure

SMS is not secure and smartphones can be infected. Exploits with inherent protocols such as IMSI catchers and signalling system no 7 can circumvent.

Operational Discipline is Mandatory!

The system should provide: no self-enrollment, secure offsite backup, instant disaster recovery and graded privileges for different administrator roles.

Identity Assurance for Pulse Connect Secure

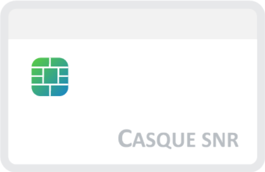
Need secure components with no dependence on third party libraries – CASQUE SNR has its own Challenge/Response protocol that provides Authentication, Key Update and Key Management for Pulse Connect Secure VPN users.

CASQUE SNR Tokens

OPTICAL TOKEN

Receives Challenge from any Screen uses pattern recognition, automatically adjusts for changing brightness

SMARTCARD TOKEN



Receives Challenge from any standard contact Reader, or can use wireless NFC communication

Solution Requirements

Secure Access Appliance

Requires PSA, MAG or virtual appliance.

Pulse Connect Secure

Appliances require software release 8.2r3 or higher.

Standalone Administration System (SAS)

Customer managed Windows PC

CASQUE SNR Authentication Server (CAS)

Windows or Linux Platform with CD and at least 1 Network port, all with latest patches

CASQUE SNR Optical Token

Any Pulse Secure supported User Client with HTML5 WebGL browser and screen of at least 5cms

CASQUE SNR Smartcard Token

Standard contact or wireless NFC capability, client requires the CASQUE SNR Player app

Benefits

Resists Clones

Dynamic Key update forces either the real token or a clone to be out of sync so the clone can't authenticate.

Prevents Insider Attacks

If a privileged insider copies the CAS Server and gives to a collaborator, there is no risk as the generation of keys cannot be replicated.

Customer is Key Custodian

The customer populates the CASQUE SNR Tokens with locally generated keys so the manufacturer or system intergrator is never part of the security risk.

Independent Validation

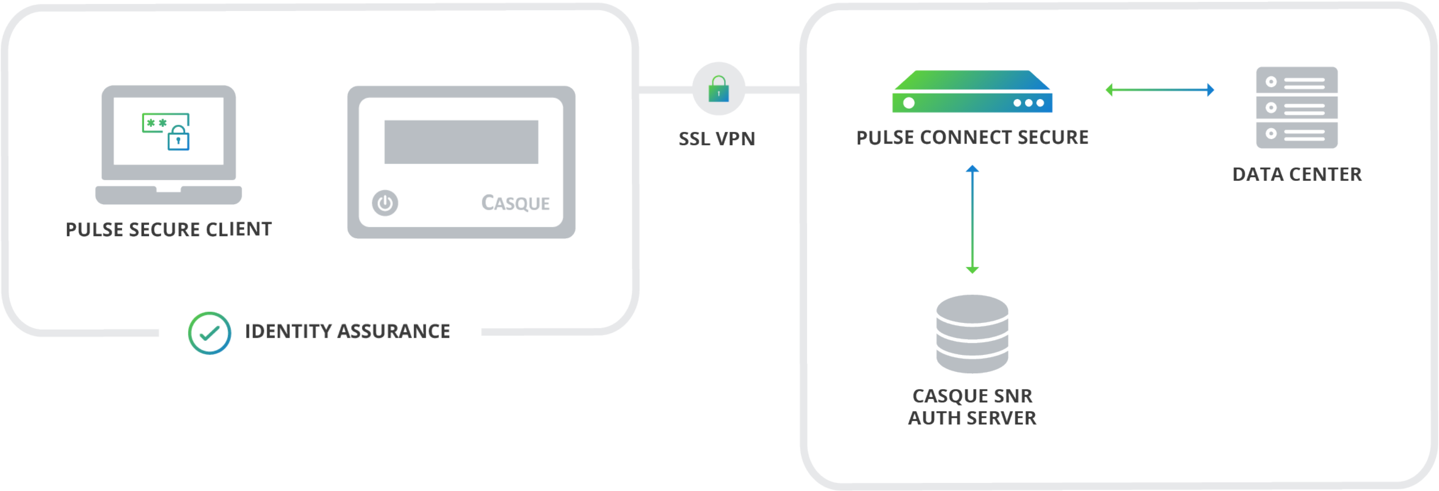
The CASQUE SNR has been source code certified by UK CESG and can be suitable for UK Government use at Secret, it is also NATO approved.

Secure Backup and Transactional Logs

Provision is made within the system for secure backup at a remote site with rapid recovery in case of failure. Each access and its outcome are logged.

Token is not a Cryptographic Item

CASQUE SNR Token *does not* contain the complete key-set. Data in the challenge message unlocks the keys allowing stored encrypted keys to be decrypted and temporarily available in dynamic memory.



How does it work?

CASQUE SNR, developed by Distributed Management Systems Ltd, is fully self-contained with no third party dependencies- it has its own Challenge/Response Protocol which is cryptographically realised using standard algorithms and provides Key Generation and Key Management. Each CASQUE SNR Token contains a secure EAL5+ rated processor. There are two types - “Optical” with its own rechargeable battery and display and “Smartcard” with both contact and wireless NFC capability. The Optical Token is truly client-less. The Smartcard requires a Client Player. Alternatively, the Challenge can be presented as a QR code on any Screen and snapped by an Android Smartphone with the CASQUE SNR NFC Token.

Managed Service Capability

A CASQUE SNR Token can, at the SAS, have all its keys completely replaced; Tokens so refreshed can be allocated to different Client

Short Messaging

There is provision for short text or hex messages to be sent to the Token enabling secure delivery of part keys or command control codes

Internet of Things

CASQUE SNR Smartcard Sims can be attached to intelligent “Things” allowing Mutual Authentication and peer group secure communications

Case Study Military Grade

The UK Ministry of Defence relies 24/7 on CASQUE SNR for remote access applications