Fortinet – CASQUE Joint Solution Brief

Fortinet and CASQUE Security Solution

<Enterprise owned and controlled High Grade Identity Assurance>

Distributed Management Systems has developed CASQUE, a radical, Identity Assurance Technology. The inherent vulnerability with existing Multi-factor Authentication products is that they rely on fixed secrets. This could be an embedded key that manufacturer inserts in a one off password generator or the private key that attests the credibility of a FIDO2 type dongle.
If found out by discovery, or by quantum factorisation or more likely, disclosure from a privileged Insider; the security is bust.

Fashionable software only solutions such as applying machine learning to define usage profiles and thereby deny access on exceptions have intrinsic flaws. The most permissive become the easiest targets and you have to have an administrative team on call to handle legitimate exceptions-but how are these policed?

CASQUE is the only Multi-factor Authentication Technology that does not rely on fixed secrets, so there is nothing for a hacker to target or for an Insider to disclose.
CASQUE therefore removes a whole segment of threat vulnerability. Moreover, because it denies Users possible reasons to support their repudiation of access, it acts as a powerful deterrent against collusion.

CASQUE and Fortinet recently established a technology partnership to address the above challenges. The joint solution protects the Enterprise's digital crown jewels, prevents Insider collusion, and acts as a potent deterrent to user misuse and so reduces the overall risk to the Organisation.

Joint Solution Benefits

- Allows Customers - not third parties - to own and manage their Identity Access.
- Enables Customers to setup an independent, federated, high grade Identity Management ecosystem with secure access to web/mobile applications hosted across on-premises and multiple cloud environments.
- Denies Users the ability to repudiate illegal access and so acts as a powerful deterrent.
- Removes a substantial segment of threat vulnerability since there is no fixed secret to be targeted by Hackers or be disclosed by corrupt Insiders, moreover Tokens cannot be cloned.

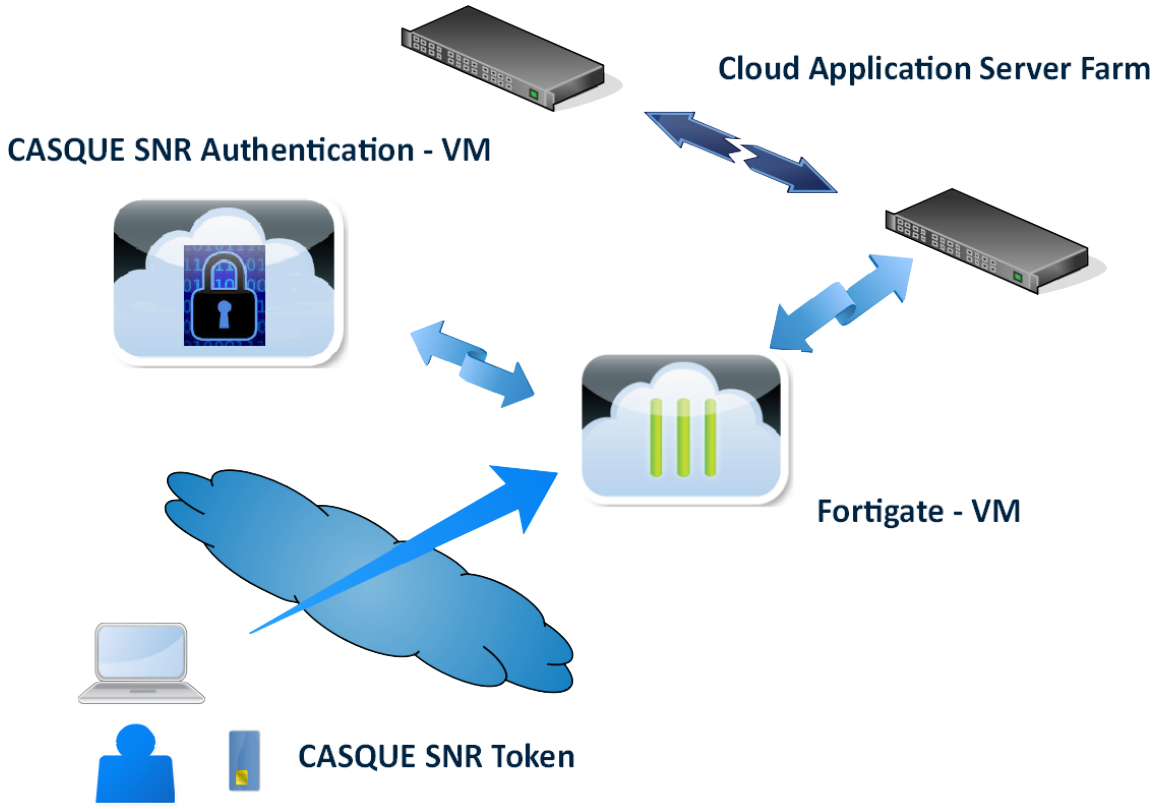
Joint Solution Description

CASQUE is based on a Challenge-Response Protocol with the User needing a secure hardware chip to make the response which enables dynamic key change. There are many manifestation of the handheld Token; the most popular being an EAL6 rated secure contactless smartcard.

There are two main software components; the first enables the Customer to populate Tokens with initial key sets and the second is the CASQUE Server that provides federated Authentication services to the Fortigate Gateway.

The architecture of the joint solution is summarized in the illustration below.

Diagram of Joint Solution



Use Cases

Current activities in many Organisations include both transforming legacy systems as well as developing new applications into Cloud deployments with the capability of mobile access.
The pertinent and obvious questions include:

How are the Administrators of the cloud deployment controlled?

Do they use authentication products that have inherent vulnerabilities - note that the small print in cloud providers management service contracts usually deny all liability for any data loss.

If you have multiple Cloud providers or move to a new Cloud provider do you have to reinstate Identity provision?

Who generates and can read your keys? With CASQUE only the Customer generates and controls keys.

If a Token is reported lost, can it be instantly suspended? FIDO2 and Google Titan fobs have no association with Users, so lost devices still work.

Are tokens able to be securely and easily redeployed for different users and systems?
Most users want access from a set of different devices- mobile, laptop, desktop with different operating systems- android, windows, linux. CASQUE can provide a universal solution by delivering the challenge directly to a mobile when the mobile is the client; or displaying it as a QR coded image with the mobile acting as a surrogate reader.

CASQUE is predicated on the Fortress design - extensive boundary walls but with the inner keep, containing the digital Crown Jewels, having the strongest and thickness walls - the CASQUE barrier.

CASQUE does not seek to replace existing security provision but to strategically augment it.
It is foolhardy to use a known vulnerable method to protect administrator access which, if it can be breached, results in the ruination of the entire integrity of the cloud platform including exposure of the crown jewels.

About Distributed Management Systems

CASQUE Technology has been developed by Distributed Management Systems, a private company owned by its Directors and based in Lancashire, England.
CASQUE has granted US and EU patents and is certified by UK National Cyber Security Centre as suitable for Secret.

Learn more at < **https://www.casque.co.uk** >