High Grade Identity Assurance for the Cloud

This presentation shows how CASQUE provides Enterprise owned and controlled, high grade, federated, Identity Assurance for Web Applications

"It is foolhardy to use an authentication method with a known vulnerability to protect access which, if breached, results in the integrity of the entire Cloud platform being compromised"

Data breaches continue to proliferate !

1,334,488,724 breached records worldwide in April 2019.

Running annual total 5.64 billion

Monthly average 1.46 billion!

(IT Governance)

Why Data Breaches Continue to Proliferate?

1. Existing Authentication Methods are vulnerable
2. Users can easily deny access so feel able to disclose or be complicit
3. Users are ill-disciplined
4. Weakness in IT infrastructure design, implementation and control

CASQUE can solve [1] and [2]

The Problem

Common Out-of-Band Authentication Methods like SMS, Email are weak with OTP only slightly better*

Products** exploiting such vulnerabilities are publicly available

* NIST Digital Identity Guidelines NIST.SP.800-63b.pdf

** Stingray, Shylock

Vulnerabilities

Current multi-factor authentication (MFA) methods have exploitable weaknesses – they rely on fixed secrets

- Password, Embedded key in SecurID
- Private key in PKI infrastructure, Attestation key in FIDO2
- Algorithm and data points used in zero knowledge methods

If discovered by hacking, calculated or disclosed by Insiders,

the security is bust!

Software Only Authentication – *instrinsic flaws*

Do not be beguiled by “Adaptive” software only methods such User profiling

- Most privileged Users tend to need the most permissive usage characteristics so become the easiest target
- Need 24/7 administrative team to handle legitimate exceptions - how are they authenticated?
- Would not be certified by NIST at High Assurance because it cannot distinguish illegal access - User can always plead the repudiation defence

"Someone has watched my behaviour and got in"

The Solution

Solve the weak authentication problem

- **keep changing the secret!**

But very difficult to acheive

- Indeterminacy
- Outage & Recovery
- Replay Attack

The Solution

We have developed a radical Challenge-Response Protocol

- User has handheld Token containing a secure chip
- Secure chip has EAL 6, FIPS 140-2 Level 3 Assurance

The Solution

CASQUE Challenge-Response Protocol

- Dynamic key change
- Nothing for a hacker to target or for an insider to disclose
- No token clones

The Solution

Keep changing the Secret -- needed 4 inventions!

- One has Granted US & EU patents *
- NATO approved, in use 24/7 by UK MOD
- Certified by NCSC as suitable for Secret ** - the only such
- Easily fulfils NIST Level 3 requirements - the highest

* https://patents.google.com/patent/WO2013132224A3/en
** https://www.ncsc.gov.uk

The Solution

Token has many manifestations

Optical Token

USB Token

Contactless Smartcard

Contact Bluetooth Smartcard

Surrogate Camera Token

Different forms for Client and Clientless applications

The Business Case

Digital Transformation: Cloud and Mobile

- Who polices the administrators of your Cloud deployment?
- Can an Insider reveal access secrets?
- Who is liable if a breach occurs?
- (certainly not the Cloud Provider)
- How is the mobile User authenticated?
- Are they authenticated by vulnerable methods?

The Business Case

Digital Transformation: Cloud and Mobile

- Who controls the Identity Provision?
- Can a User or Token be instantly suspended?
- (FIDO2, Google Titan have no knowledge of the User)
- Are third parties part of the risk?
- Are Tokens be reusable?

The Business Case

Federated High Grade Identity & Access Management

- Users - not third parties - should own and manage Identity Access.
- Need to determine and segregate data that is vital - “Crown Jewels”
- Access to the Crown Jewels must have highest Identity Assurance

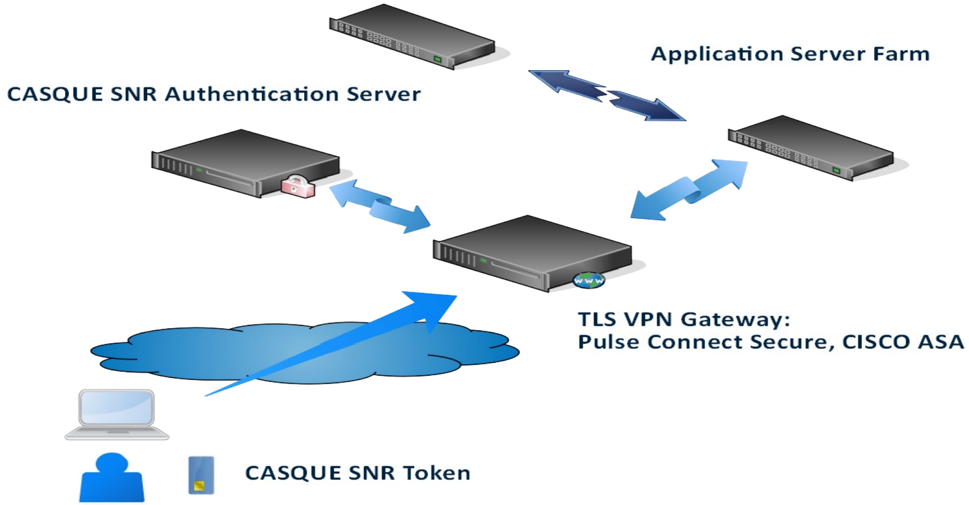
Digital Transformation: Cloud and Mobile

Access required from several devices

CASQUE universal solution delivers challenge directly to mobile if it is the client or presents as a QR coded image on a laptop screen with the mobile’s camera acting as a surrogate Token reader

[Click to see the User experience in this movie]

The Business Case – *Integrates with Gateways*


Application Server Farm
CASQUE SNR Authentication Server
TLS VPN Gateway:
Pulse Connect Secure, CISCO ASA
CASQUE SNR Token

Jointly developed Integration with main Gateways including Pulse Secure, CISCO, Fortinet

WSO2 Identity Server - Capabilities

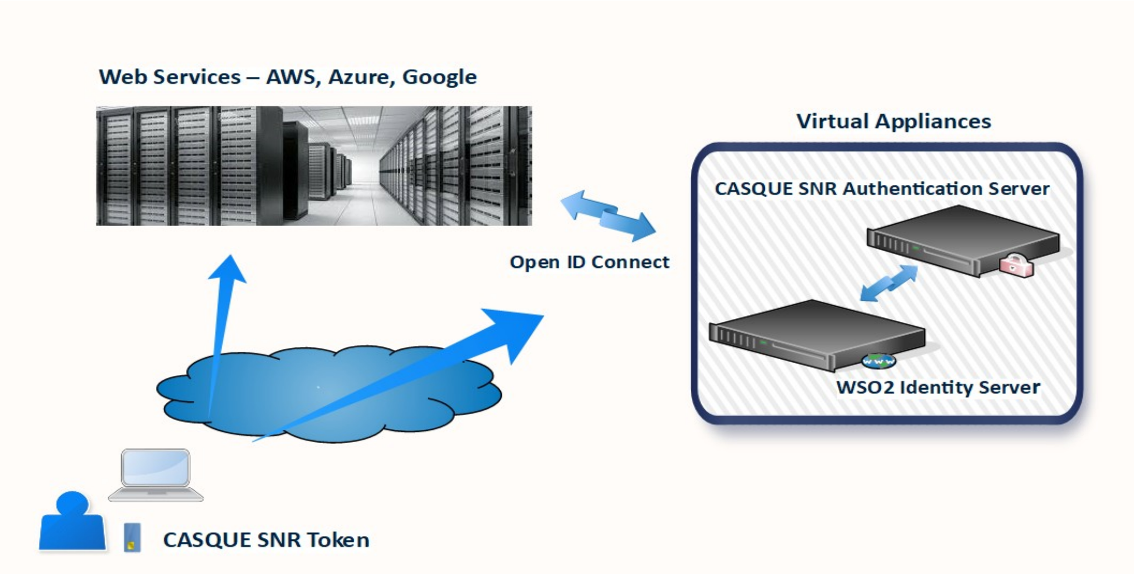
WSO2 is an open source, open standards IAM product for identity federation and single sign-on (SSO)

- Identity Federation and SSO
- Identity Bridging
- Account management & Identity Provisioning
- Access & Authorisation Controls
- APIs & Microservices security
- Privacy & Identity Analytics

CASQUE with WSO2 Identity Server

- Enables Administrators to setup a federated Identity management ecosystem and secure access to web/mobile applications & endpoints across on-premises & cloud environments
- Jointly developed CASQUE Integation has greater functional capability than DUO, PING, OKTA and RSA - and can be cheaper !

The Business Case - *complete IAM provision*

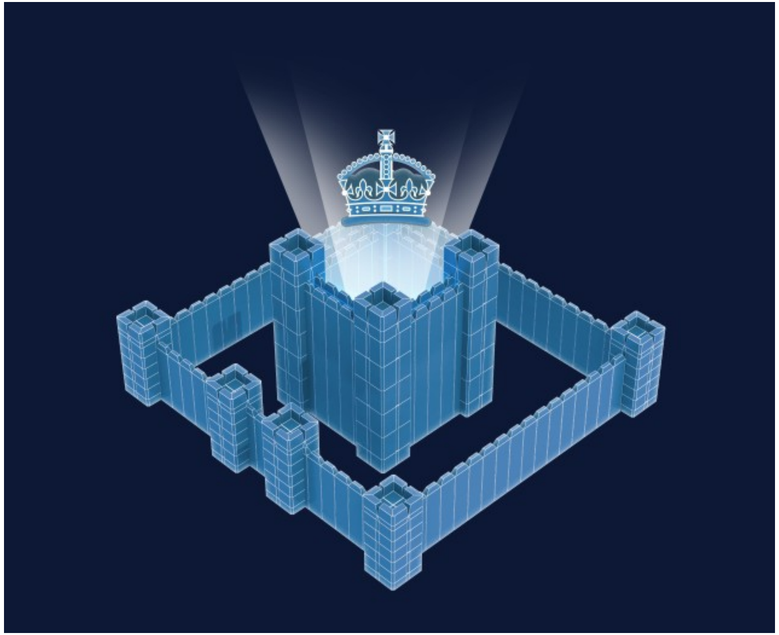


Federated, User controlled, High Grade Identity Assurance for a Cloud of Web Applications

Most Economic way to reduce overall Risk

CASQUE

- co-exist with existing security
- Protects the crown jewels
- Reduces overall risk *economically*



Most Economic way to reduce overall Risk

“It is foolhardy to use an authentication method with a known vulnerability to protect access which, if breached, results in the integrity of the entire Cloud platform being compromised”