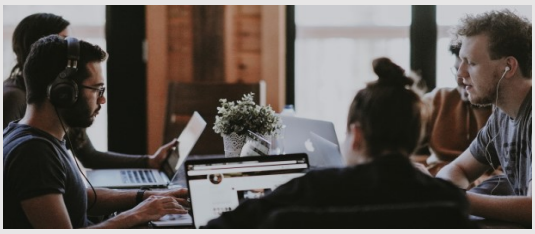
# Pros & Cons of Identity as a Service

# CASQUE

# The *high-grade* Identity as a Service

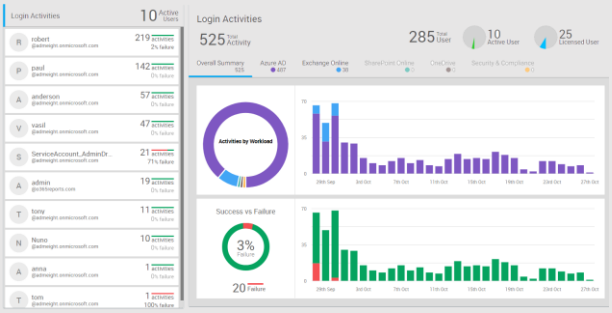
## Unlock the Power of federated Identity as a Service for Your Organization



Why struggle with ad hoc, complex identity management when you can streamline and secure your operations with CASQUE, the high–grade Identity as a Service Platform

## Simplified Identity Management Made Easy

Centralized platform for seamless user identity management
Effortlessly manage access controls and authentication mechanisms
Reduce administrative burden and focus on core business activities



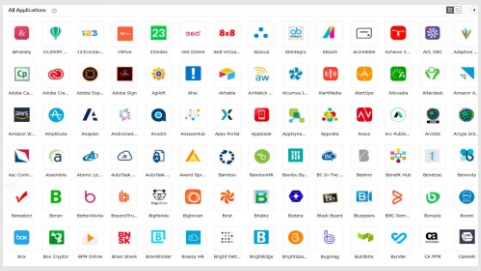

## Enhanced Security for Peace of Mind

Robust security measures to protect user identities and sensitive data
Advanced authentication methods, including high-grade multi-factor authentication
Stay ahead of unauthorized access and mitigate security risks

## Scalability and Flexibility to Adapt

Seamlessly accommodate a growing number of users and applications
Easily add or remove users, provision access rights, and manage privileges
Scale effortlessly to support rapid growth or business fluctuations

## Experience the Convenience of Single Sign-On



Access multiple applications and services with a single set of login credentials
Improve convenience and user experience
Reduce the risk of weak or reused passwords

CASQUE

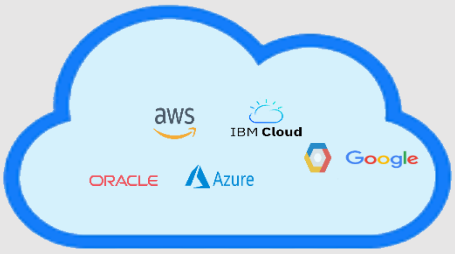
# The *high-grade* Identity as a Service

## Ensure Compliance and Governance

Achieve regulatory compliance and adhere to industry standards
Features for identity lifecycle management, audit trails, and access certifications
Demonstrate your commitment to data privacy and security

## Seamless Integration with Cloud Services

Securely authenticate and access cloud resources from anywhere
Connect with various cloud service providers effortlessly
Stay productive regardless of location, device, or network




## Cost Savings and Predictable Operational Costs

Eliminate the need for expensive in-house infrastructure
Reduce upfront capital expenditures and maintenance costs
Enjoy the benefits of an adaptive subscription-based model

## Boost User Experience and Productivity

Seamless and intuitive authentication process
Minimize access management friction for enhanced productivity
Empower employees to focus on their tasks and deliver results

## Rapid Deployment for Immediate Impact

Quick implementation to start managing user identities and access controls
Gain instant access management capabilities
Experience agility and flexibility in your operations

CASQUE

# The Challenges of Identity as a Service

## Risk of Compromise

*Breaches continue to proliferate. Two difficult, and until now, intractable problems are likelihood of attack by Insider collusion and the damage that ensues whilst breaches remain undetected - this "Exposure Time" currently averages 9 months!*
*The main enabler for these problems is the vulnerability of current methods of User Authentication whose weaknesses provides convenient excuses for disaffected Insiders to deny their, or their collaborators, illegitimate access.*
*The bigger the organisation the more likely to have a disaffected employee or subcontractor driven by the persistent human frailties of Ideology, Revenge and Greed.*
*Is the access vulnerable? Existing Multi-factor Authentication Methods rely on keeping fixed secrets such as an embedded key in a Token or the Private Key in a PKI structure. If these secrets are discovered or, more likely, revealed by a complicit Insider then the security fails.*

**CASQUE has a Challenge Response protocol with the User having a highly secure chip with code on it to respond to the Challenge. The Challenge delivers key changes at each User interaction so there is nothing fixed for a hacker to target or for an Insider to disclose.**
**CASQUE makes identification of clone attempts immediately known and recoverable.**

## Availability

*Dependence on the Supplier to perform and ensure resilience is an obvious concern*

**CASQUE has inbuilt dynamic backup capability that can take advantage of the Cloud's geographic locations or indeed be housed in the Customer's own domain.**
**CASQUE does not rely on any third-party IP or external software libraries so a complete deposit can be made available from Escrow if severe non-performance of service level agreement occurs.**

## Privacy

*Does the Identity application require User identifiable information like email addresses and mobile numbers? Does the on-boarding process allow self-provisioning?*

**There is no self-provisioning and its associated abuse potential with CASQUE. The Customer dispatches the CASQUE Tokens personally to Users. Users who report loss can have their access immediately suspended.**

## Integration

*How easy is it to graft the Identity technology onto existing applications and User directories?*

**CASQUE uses the Open ID Connect protocol which is widely adopted by the main Cloud providers as well as web services such as WordPress and Microsoft Power Pages and Apps.**
**CASQUE has closely coupled integrations with both WSO2 and Curity Identity Servers allowing Single Sign On and directory integration.**

## Cost

*What are the cost implications?*

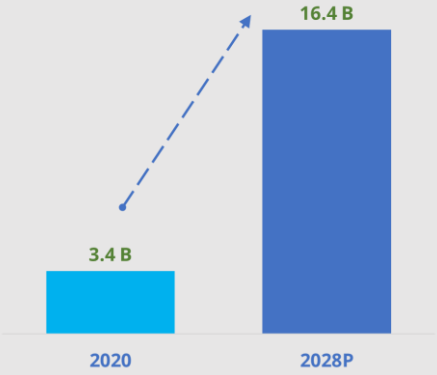
**Adaptive Authentication determination allows discretion in choosing whether CASQUE is used just for the most privileged group access. Flexible monthly subscription means no upfront capital costs are required.**

CASQUE

# We can make you stand out

*and be outstanding*

**Identity as a Service is growing – do you want get the Benefits?**

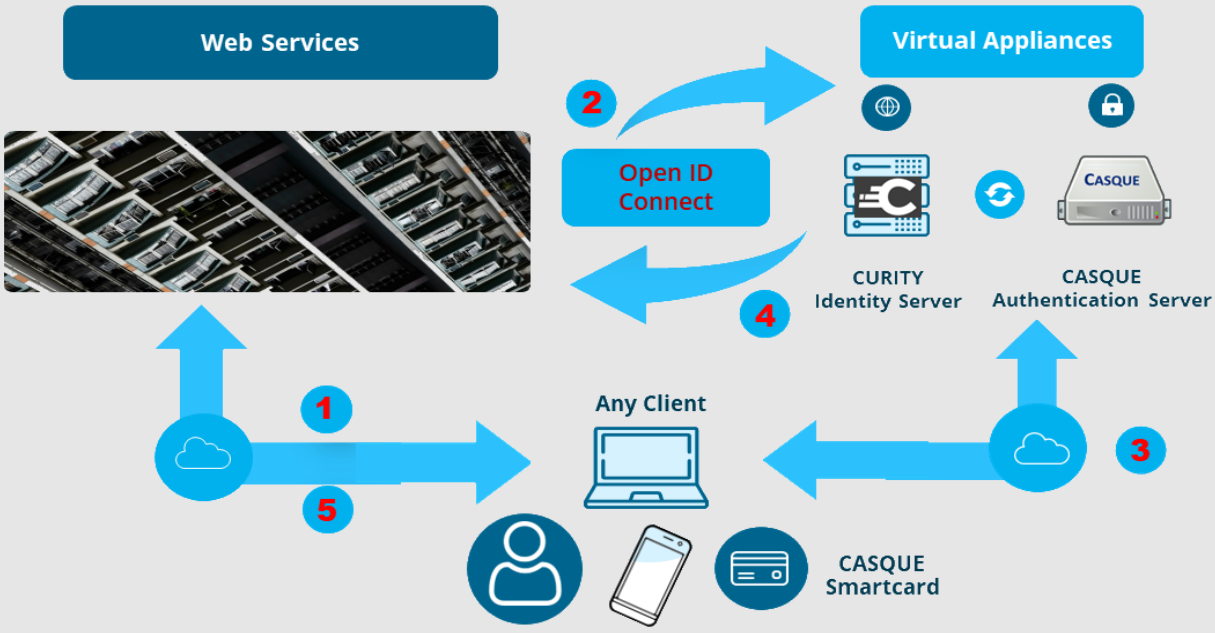



**Works on all clients- Windows, Linux, Mobile with no need for card readers**

**CASQUE has no secret to hack or disclose**

**Zero Trust Access with Zero Vulnerability**

**Universal Solution- AWS, Azure, Google Cloud, WordPress Sites, Microsoft Power Pages, Apps**



CASQUE

# Features and Benefits

01

## Detect Compromise

Continual Key change makes cloning of Tokens immediately visible. No doubt when malfeasance occurred.

02

## User Attribution

No self-provisioning weakness. All attempted access recorded against specific Users. Additional credentials tie User to Token.

03

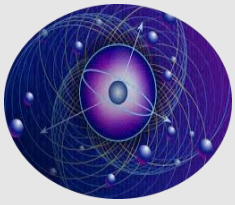
## Insider Deterrent

Corrupt Insiders cannot make excuses to repudiate their access so is a powerful deterrent against Insider collusion.

04

## Quantum Computing Immunity

No Public Private Key dependency so no possible factorization susceptibility.



05

## IP Sovereignty

No dependency on third party IP or software libraries so no supply chain vulnerability. Source code is available.

CASQUE

# Features and Benefits

06

## Customer Ownership

No need to give User identifiable Information to third parties. Customer isin complete control of Authentication Server

07

## Out-of-Box Integrations

Mutually tested integrations with major Gateway Manufacturers such CISCO, Juniper, Pulse Secure, Fortinet

08

## Federated Identity Provider

Ideally suited to acting as Independent Federated Identity Provider controlling access wherever critical IT resources reside.

09

## NIST High Grade Security

Easily satisfies all the NIST criteria for highest Assurance level without needing support from other methods.

10

## Multi-Function Capability

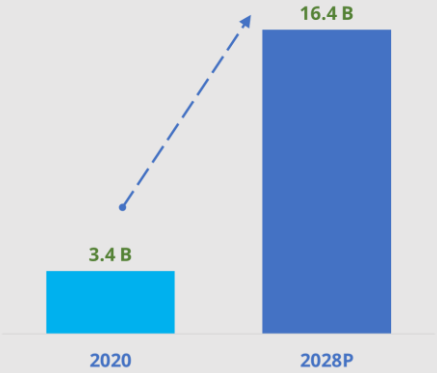
Does not disturb existing Authentication methods. CASQUE Token can be resident on Java Card alongside other credentials.

# CASQUE

## We can make you stand out

## *and be outstanding*

**Identity as a Service is growing – do you want get the Benefits?**




**Works on all clients- Windows, Linux, Mobile with no need for card readers**

**CASQUE has no secret to hack or disclose**

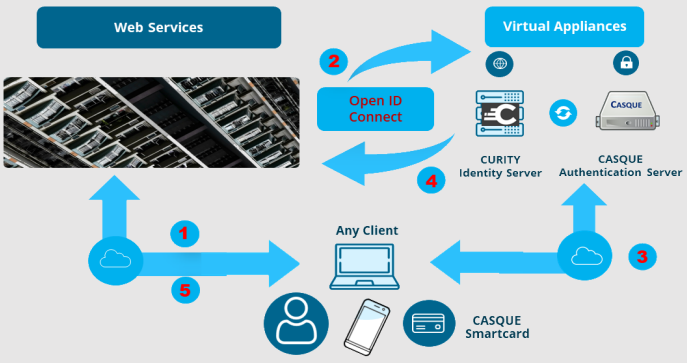
**Zero Trust Access with Zero Vulnerability**

**Universal Solution- AWS, Azure, Google Cloud, WordPress Sites, Microsoft Power Pages, Apps**

**NIST High Grade Security**

**Insider Deterrent**

**Detect Compromise**




**User Attribution**

**Customer Ownership**

**Multi-function Capability**

**Out-of-box Integrations**

**Quantum Computing Immunity**