The Case against Adaptive Authentication

We believe the fashionable trend for “Adaptive Authentication” where Identity is determined by a software only technique based on the User’s “Use Profile” is flawed both in design principle and operation.

The User’s Use Profile is usually determined by the usual geographic location, times of access, client device recognition- e.g. browser type, OS etc.
Clearly the more profile data and the more frequent updating is better but this demands a large database and its housekeeping- how is this maintained and protected?

The nature of fast growing Enterprises means that the higher privileged Users commonly have the more dynamic Use Profiles. If a Senior Executive has to attend, at short notice, a new Customer meeting tomorrow morning in Morocco or the Support Analyst on duty is indisposed and a substitute has to be quickly got then an Administrator has to be called and how is their Identity protected- can they change anything at any time irrespective of where they happen to be?

The attraction of not having a hardware token will soon diminish if high ranking Executives get frustrated by cumbersome exception handling and the only resulting solution will be to reduce the restrictions on the very Users who need the most flexible, privileged access rights.

Operational weakness is inherent in the case of Insider collusion that discloses login and profile details. The Insider threat is pernicious because of the human motivations of revenge, ideology and greed are persistent. If the User can easily deny their access then they feel they can get away with complicit arrangements.

In CA Technologies 2018 Insider Report, a majority of Organisations interviewed confirmed insider attacks in the previous 12 months.
Unfortunately, it does not help when publicly available apps exist to fake geographic locations:

Our design principle in contrast, is both economical and efficient and is based on the “Fortress Construction”-have thin, functional outer walls (keep your existing security barriers) but have very thick, impenetrable inner keep walls. This type of construction is not new *but is proven*.
By strongly protecting the access to really important assets you diminish the total risk.

Migrating internal, legacy systems to the Cloud gives the opportunity to re-evaluate what are the Organisation’s key data assets, where should they reside and who should have access to them. Who should have access to the important aggregated data or new product development tests. This subset forms the CASQUE SNR Users.

Since CASQUE SNR does not rely on fixed secrets/keys there is nothing to be discovered by hacking or by disclosure from a malevolent Insider.

US NIST Digital Identity Guidelines document maintains that software only products can never be considered for providing the Highest Assurance Level- a criteria that CASQUE SNR easily fulfills.