# Zimbra Integration with CASQUE SNR Authentication

Zimbra Collaboration is the world's leading open source messaging and collaboration solution, trusted by more than 5,000 companies and public sector customers with over 500 million end users in over 140 countries. Capabilities include email, contacts, calendar, file-sharing, video conferencing and task coordination which can be accessed from via any device. Zimbra can be on premises or self-hosted.

The requirement to complement this strategic investment with appropriate access security is obvious but there is no need to compromise using "weak" two-factor authentication products that use fixed secrets, which when discovered or disclosed, render the system vulnerable. SMS is not secure and smartphones can be infected-exploits with inherent protocols such as IMSI catchers and signalling system no 7 can circumvent.

NIST Special Publication 800-63B, "*Digital Identity Guidelines, Authentication and Lifecycle Management*" dated June 2017 makes interesting reading; it places out of band (e.g. SMS messages) in the lowest category of Authentication Assurance Levels with OTP (e.g. SecurID) only slightly better.

CASQUE SNR easily fulfils the criteria of a "Multi-factor Hardware Crypto Device" as defined in NIST 800-63B and so is able to be employed for applications demanding the highest assurance level *without requiring multiple other methods for support*. It is the only Multi-factor Authentication product certified by UK's NCSC as suitable for secret and is NATO approved.

CASQUE SNR uses a Challenge-Response technique to change keys dynamically and invisibly, removing fixed targets and so is immune to insider attacks, token clones and manufacturer reveal. Both Client and Clientless solutions are available with the User Token based on an EAL5+ secure chip. There is a choice of Token form including Optical, Contactless Smartcard and Bluetooth Fob. In the latter case, the Token is tied cryptographically to a specific Client and will respond the CASQUE SNR challenge without the need for the User to type anything extra other than their normal credentials.

CASQUE SNR for Zimbra comprises a dedicated Server as the User landing site with a CASQUE SNR Authentication Server as its Back End. After successful completion of the Challenge–Response interaction, the User is referred to the Zimbra Server with the appropriate SAML Token.