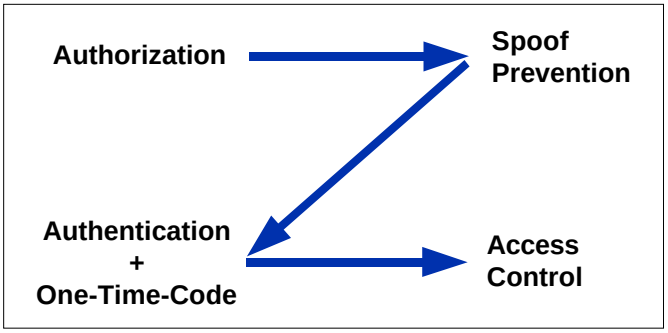
nma.com/zsentry/

Request a ZSentryID trial

ZSentryID™

Two-Factor Two-Channel User Authentication One-Time-Codes Through The User's Mobile Phone

ZSentryID ensures that only authorized users are allowed entry to your network, even if a user's credentials are compromised. ZSentryID extends the security, cost, scalability and zero footprint benefits of NMA ZSentry user authentication technology to two-channel authentication with dynamically generated, unpredictable, one-time codes.



Reduces Costs And Is Compatible With Your Infrastructure

ZSentryID takes advantage of mobile phones and pagers — devices that users already have and know how to use — to send the one-time authentication code required from a user. There are no mandatory renewal costs. By means of plug-ins supplied free of charge by NMA, your existing firewalls, network access servers, VPNs and Web applications can readily support ZSentryID two-factor two-channel authentication.

Flexibility For Secure Access Without Mobile Service

You have the flexibility to combine ZSentryID with ZSentry, allowing access to some resources to be controlled by two-factor authentication without a dynamically-generated one-time code. This can be useful as a fall-back in case there is no mobile phone service, no pager service, or as another access class. ZSentry provides two-factor strong authentication without password lists, shared secrets, PINs, and databases. See nma.com/zsentry/ or our ZSentry brochure.

User Authentication Where And How You Need It

ZSentryID can be used by your employees, business partners and customers, whether local, remote or mobile, to authenticate access to VPNs, 802.11 LANs, remote access applications, network access servers, file servers, extranets, Web servers or local applications.

Hard For Hackers, Hard For Internal Attacks

User authentication to the ZSentryID server is protected by TLS/SSL. The TimeCode is generated by the ZSentryID server using a 128-bit key and the local time, and is statistically unique. The TimeCode is sent to the user's pre-registered mobile phone using A5 encryption and expires in a short time, for example, 60 seconds. No one, not even the ZSentryID server, has a record of which TimeCode is valid for each user — which prevents attacks and allows redundant ZSentryID servers to be easily deployed for scalability purposes. In addition, the user's TimeCode must be entered using the same TimeCode entry page that was sent to that user's browser, preventing the use of intercepted TimeCodes. User authentication cannot be silently compromised.

Two Channels Develop Trust And Close The Loop

ZSentryID uses two, independent, encrypted communication channels (web browser using TLS/SSL encryption or WAP microbrowser using WTLS encryption, and mobile phone with text messaging using the A5 encryption protocol) to both develop trust and close the loop on the user's identity before connecting the user to a controlled resource — directly or, for example, by means of a network access server.

Easy for the User

Through a browser, a user presents a valid ZSentryID ZCode and Password to a ZSentryID server. The ZSentryID server then dynamically generates a one-time, unpredictable TimeCode that is sent to the user's pre-registered mobile phone, either as an SMS text message or as an email. A TimeCode entry page is sent to the user's browser, asking the user to complete the authentication process. Before entering the TimeCode, the user may verify a ReturnCode provided on the TimeCode entry page, to prevent server spoofing. Typically, the user has 60 seconds to enter the TimeCode.