2FA

Triangle Solutions b.v.

Situation:
When implementing VDSS, there is an increasing pressure/demand from the customer to deliver 2FA.

Research questions:
Can you list the pros and cons for each factor?
Which factor(s) can we best use for this?
Do you have further advice for us how we can apply 2FA?

Supporting information:
Two factor authentication (or multifactor authentication) consists of multiple factors of authenticating according to veridiumid.com.

Duo writes that there are five popular factors that users can identify with. It says that factors are pieces of information that a user can provide to verify his or her identity. The following five authentication factors are listed by duo: the knowledge factor, the ownership factor, the biometric factor, the time factor and the location factor.

- **Knowledge factor:** One can use a password to login. Some applications offer a security question in case the user has forgotten his or her password.

- **Ownership factor:** This includes all physical objects. Examples he mentions are: keys, mobile phones, smart cards and tokens.

- **Biometric factor:** This includes the human body. Examples he named are: fingerprints, iris scan, facial recognition or voice recognition.

- **Time factor (OTP):** By looking at what time and on which day the user logs in, it can be assessed whether the login attempt needs additional validation. If a login attempt deviates from the normal schedule, the user will have to take an extra step to identify himself.

- **Location factor:** By using GPS, an IP range or other methods, the location of the user can be traced. The term "location" can refer to the physical location of the user, but it can also be, for example, a local IP address within the intranet.