DTS
Multi Factor authentication

Multi Factor authentication

Many employees use exactly one password, which is considered sufficient. However, passwords can be intercepted, read or hacked. Nothing then stands in the way of third-party access. With cloud-based, market-leading SafeNet multi-factor authentication, we eliminate this risk and protect you from unauthorized access.

- Multi-factor authentication for remote protection, third-party access protection and protection of data, networks, applications & the cloud

- Customized authenticators

- Maximum convenience through extensive, simple automation

- DTS managed services, including 24/7 support

Thales/SafeNet is a leading global provider of IT security solutions. Authentication solutions strengthen VPN security for remote access, protect data on laptops and PCs, enhance network access security and simplify password management and protection. This is made possible by a wide range of authenticators, management platforms and security applications.

2-factor authentication secures proof of identity for all users, for every device with network access and for every application, using a combination of two independent factors. If you want to withdraw cash, you need a card and a PIN. With SafeNet Authentication Service (SAS), you also identify yourself with a password and an additional, flexible, token option, tailored to your needs and wishes. You have hardware, software, multi-platform tokens, SMS or token-free options to choose from. The solution also offers vendor-independent token integration with comprehensive APIs. Of course, the appropriate token is also available on a rental basis and it can be passed on to another user at any time. With easy rollout, simple reconfiguration and an unlimited lifetime, there are suitable authenticators for every type of user. If a token is lost, a temporary software authenticator is quickly issued.

The comprehensive automation of the SAS also significantly reduces the work involved in provisioning, administration, authentication rules and user and token management. Automated policies, including for pre-authentication and exception-based management, provide intelligent authorization and real access control, as do alert settings.

Further user satisfaction is provided by comprehensive self-service functions, push & pull of soft tokens and token-free methods. You can also generate automated reports for IT compliance, audits, accounting, or to meet key security standards such as SOX, PCI and HIPAA. The SAS does not entail any additional or hidden costs.

1

User opens resource, and enters their username

2

User gets push notification, and taps to approve the login request

3

User is logged in to the protected resource