Mideye

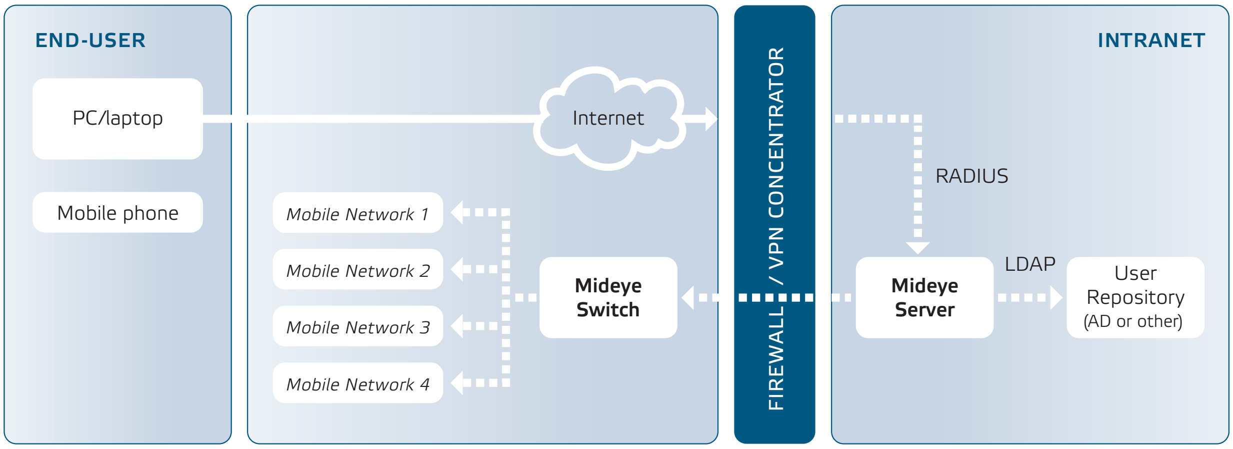
Using the mobile phone as a security token

The Mideye Authentication Service

A key issue for enterprises enabling remote access to sensitive information is how to establish the identity of the end-user. Mideye Authentication enhances the strength of remote authentication by using the mobile phone as an extra level of security.

The Mideye Authentication Service provides strong two factor authentication by using the mobile phone as a security token. In situations when an end-user requests access to a protected application, the user is asked to enter a secret password together with a one-time password that is presented on the user's mobile phone. Mideye protection can be deployed for different applications:

- ▶ **INTRANET ACCESS** Secure intranet access via VPN (IPsec or SSL), dial-up or a thin client.
- ▶ **EXTRANET ACCESS** Restricted access to protected extranet services via a web portal.
- ▶ **CONSUMER SERVICES** Internet access to protected consumer services.



Benefits with Mideye

- ▶ *Enhanced security:* The end-user must know the secret password and be in possession of the mobile phone in order to gain access.
- ▶ *Zero footprint:* No need for additional hardware or software on the client's side.
- ▶ *Reduced costs:* No need to invest in, distribute or administer additional client hardware or software.
- ▶ *Simplified user administration:* End-user data can be read directly from an existing LDAP directory.
- ▶ *User friendliness:* Simple and intuitive user authentication dialogue.
- ▶ *Token card support:* For users without a mobile phone, the Mideye Authentication Service also supports token cards.
- ▶ *Smartphone apps:* Enable login outside of network coverage.

What is required to implement Mideye protection?

- ▶ Installation of a Mideye Authentication Server on the corporate Intranet.
- ▶ Integration with existing access products, e.g. VPN gateways or Extranet portals.
- ▶ Read-only access to an existing LDAP directory (optional).
- ▶ Internet connection to a Mideye Switch.

THE MIDEYE SERVER

Supported platforms

- ▶ Windows Server.
- ▶ Linux (Red Hat, CentOS).

Third-party software

- ▶ Database: Microsoft SQL or MySQL.

End-user data

- ▶ Read from existing LDAP repositories (e.g. AD, eDirectory or other).
- ▶ User data in the internal database as an alternative to LDAP.

Integration with Access Products

- ▶ Standard RADIUS (RFC 2865) for integration with VPN-concentrators, firewalls, access portals, etc.
- ▶ Proprietary API for custom integrations.

Operation and maintenance

- ▶ Web GUI for operation, administration and maintenance.
- ▶ Graphical user interface for server configuration.

Delivery of one-time passwords

TLS/SSL connection to a Mideye Switch for managed real-time delivery of one-time passwords via the mobile network.