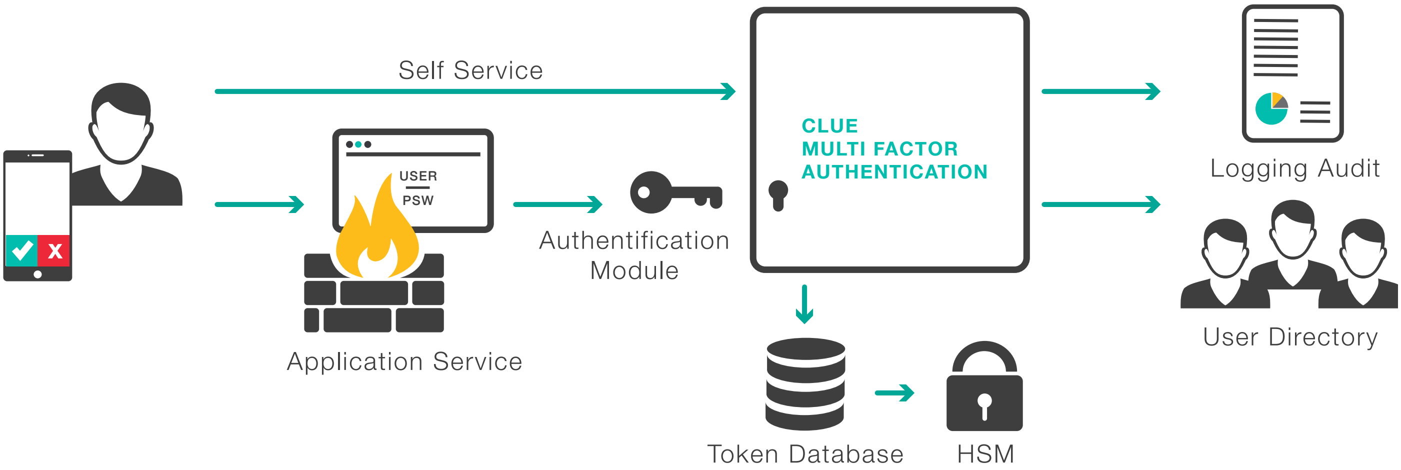
SECURITY SERVICES AG
CLUE

# MULTI FACTOR AUTHENTICATION

Clue Multi-Factor Authentication verifies the identity of users before they connect to their applications and systems. Clue Multi-Factor Authentication is easy to deploy and provides the flexibility required for secure remote access and application integration.



## A PASSWORD IS NOT ENOUGH

A single password for access protection has long been obsolete, as it is easy to crack and is full of weaknesses. Often the same passwords are used for different accesses. Thus users, unknowingly, share passwords with various providers leaving them easily exposed to theft of some sort. Often the guidelines for password creation are partly to blame. They ask for too much and encourage employees to create passwords that are, by nature, not very strong or need to be written down somewhere to be remembered.

## MULTI TOKEN MANAGEMENT

It is always useful to have an array of authentication available allowing for a “double check” of user identity or transaction. The requirements, though, for multi-factor authentication vary greatly depending on the application. We therefore support a wide range of tokens. Push Tokens provide a high level of security and significantly improve user-friendliness. QR Tokens are also very easy to use and can be integrated into Windows or MacOSX logins and applications. Whether classic with display or as FIDO U2F token, Hardware Tokens are suitable for external employees and high security requirements. Software tokens for smartphones and as text messages meet most security requirements and can be managed efficiently and cost-effectively.

## EFFICIENT MANAGEMENT

One of the biggest hurdles in the use of multi-factor authentication systems is the management of user tokens. Especially in environments where different token types are used, the rollout and operation of a token can be very time-consuming. Through the self-service portal, administration of tokens can be partially or completely transferred to the users within a defined framework. For smooth migration, pass-through tokens are available for users who have not yet been converted so that they can continue to have access as they change over to the new system.

## MULTI-FACTOR AUTHENTICATION FEATURES

### TOKEN

Our modular system allows for a broad support of token technologies and types. App tokens, hardware tokens, QR tokens, SMS and others are supported. Well documented and manufacturer-specific methods are used for token management.

### SELF SERVICE

Via a self-service portal, the user can directly introduce, activate and deactivate push tokens, app tokens and QR tokens or reset the user-pin via secure access. All possible options can be controlled with policies.

### MODULES

In addition to a RADIUS interface for remote access systems, modules for operating systems such as Windows, MacOS and Linux are available. SAML for modern authentication solutions and an API interface for direct integration into applications are also available.

### API

Through an API-First approach, unlimited possibilities in the use of Multi- Factor Authentication is made possible. Integration into your management tools, user self-service portals, products and applications, gives you full flexibility and low costs in implementation and development.

### USER DATABASES

In order to integrate seamlessly into existing IT infrastructures and applications, a large number of interfaces are supported. These include LDAP and Microsoft Active Directory. SQL- and JSON-based resolvers are available for connecting web applications.

### HSM

All confidential material is stored in encrypted form. An additional HSM (Hardware Security Module) can be used on request. This ensures that all keys are generated and managed securely and independently of your infrastructure.

## MULTI-FACTOR AUTHENTICATION SERVICE

Clue Multi-Factor Authentication enables secure deployment of remote access systems and secures access to local and cloud applications. This eliminates one of the largest attack vectors on your IT systems. Together with you, our security experts develop a suitable authentication concept and implement the necessary tools. This also includes the full operation of the required appliances, such as the regular creation of back-ups, software release and lifecycle management as well as the monitoring of health and security events.

## CLUE-LESS?

Bolster your team with Clue Managed Services. Our security experts are a welcome addition to your business. Proven products, tailor-made features and your very own personal support - we meet your requirements at a low TCO. The monthly service fee eliminates high investments and training costs, enabling you to use our services in a modular way.

## WHAT’S NEXT?

Would you like to protect to your systems and applications against unauthorized access? Do you develop applications and services and want to integrate secure authentication quickly and easily? We would be pleased to inform you off the possibilities surrounding Multi-Factor Authentication and how it can be tailor-made and securely installed in your business.