A WHITEPAPER ON NEXT-LEVEL ACCESS MANAGEMENT
# CONTENTS

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTRODUCTION</td>
<td>3</td>
</tr>
<tr>
<td>OUR MINDSET</td>
<td>4</td>
</tr>
<tr>
<td>TOPICUS KEYHUB PRINCIPLES</td>
<td>5</td>
</tr>
<tr>
<td>CENTRAUL AUTHENTICATION</td>
<td>7</td>
</tr>
<tr>
<td>DECENTRALIZED AUTHORIZATION</td>
<td>9</td>
</tr>
<tr>
<td>CONNECTIVITY</td>
<td>14</td>
</tr>
<tr>
<td>ENCRYPTION</td>
<td>14</td>
</tr>
<tr>
<td>COMPLIANCE AND ACCOUNTABILITY</td>
<td>15</td>
</tr>
<tr>
<td>AWARENESS CREATION</td>
<td>15</td>
</tr>
</tbody>
</table>
Many organisations face the challenge of granting every employee the right access to the right applications. Traditionally, an IT-department is in charge of creating accounts, assigning access rights, withdrawing those rights, and entirely disabling accounts when employees leave the company. In other words, authentication and authorisation are managed in a centralized fashion when the IT department is responsible for both.

With increasing dependency on IT systems, the pressure on IT departments increases as well. Additionally, the public debate on privacy and data protection have led to a demand for more control of access management for every organisation, further increasing this pressure.

To cope with these challenges, many organisations centralise their identity and access management even further. Specific appliances to control and monitor usage of especially privileged accounts are put in place to safeguard these vulnerable accounts. Although this increases the security of these accounts, the IT department remains in charge of access control. Especially for more dynamic organisations, centralization of access management reduces flexibility and responsibility, ultimately holding corporate success back.

Although more traditional organisations may benefit from centralizing access management, many modern companies require more flexible solutions. Fast-paced business development, self-managing teams and dynamic customers require dynamic access management. Flexible access and responsible employees, while simultaneously maintaining 100% control and accountability, are key to ensure business continuity.

This whitepaper elaborates on a new approach to identity and access management in which organisations are more secure, more manageable and with responsibilities at exactly the right levels.
OUR MINDSET

Every team or department should be responsible for access to its own IT-ecosystem, rather than a system administrator or IT-department. Access control should be fine-grained, with permissions that are easily granted and withdrawn by those responsible, in order to optimize business processes. Furthermore, the relationship between authentication and authorization must be separated: authentication identifies the user. Authentication must also be managed at a single point: anyone who requires access to any system should be identified by enforcing authentication against the same sources. Following authentication, the authorization of each user should fit the exact activities she user is entitled to perform. This requires easy acquisition of specific access when required and withdrawing this access when no longer needed. To function properly, this access must be independent of an IT-department, as the bureaucracy inherent to this dependency delays the process and introduces additional risks.
TOPICUS KEYHUB PRINCIPLES

Topicus KeyHub provides an access management solution with no need for super administrators. Having a super admin role poses a great risk to an organisation: the amount of access possessed by a super admin is both unnecessary and difficult to justify under the new GDPR (General Data Protection Regulation). When a super admin account is compromised, the entire organisation is at great risk. With Topicus KeyHub, access management is decentralized, requiring no super admins but rather different degrees of responsibility. Access Management becomes easier, more secure and creates more awareness for everyone involved.

PRINCIPLE OF LEAST PRIVILEGE

Users have no additional rights than required. No unnecessary accounts exist, and accounts are deactivated and/or deleted automatically after use. Super user admins do not exist by default. Topicus KeyHub administrators are responsible solely for the configuration of the KeyHub application itself and do not have the possibility of acquiring additional access without approval from a group manager.

ACCOUNTABILITY AND COMPLIANCE

With Topicus KeyHub, accountability and compliance follow automatically from regular usage. All systems and users are known and authenticated through KeyHub. No access can be acquired without Topicus KeyHub. Every action can be traced back to an individual, be this an employee or an external identity. The human-readable logging is self-explanatory and generates the required reports for certification and compliance within minutes.
CUSTOM GROUPS FOR SPECIFIC ACCESS

Access to servers and applications is divided into custom groups. The specific setup varies from organisation to organisation, but groundwork organises groups according to their business responsibilities. Each group is assigned a set of group managers in charge of which employees or externals are allowed access to the systems of that specific group. Groups can be created for specific clients, servers or departments and even for individual teams. All according to the requirements and structure of a specific organisation.

FORMER EMPLOYEES

If employees leave a specific team, a group manager can remove them from specific groups in Topicus KeyHub (if they haven’t removed themselves). Employees who have left the company are either disabled in the identity provider or disabled in Topicus KeyHub. Consequently former employees no longer have access to anything within the organisation.
CENTRAL AUTHENTICATION

Topicus KeyHub functions as a central point of authentication for all individuals, both internal and external employees. Access to systems and/or passwords can only be gained following authentication. Authentication can be done using several identity providers over various protocols. Whether an organisation has an Active Directory in place, or has all identities in an HR-application or Google directory, Topicus KeyHub verifies the identity of each user against the specific identity provider(s).

If no source of specific identities is present, Topicus KeyHub has an internal directory which can be used as well. For example, accounts for contractors and auditors requiring access can be stored in the KeyHub-directory.

When an employee leaves the organisation, all access rights are automatically revoked when the account is disabled in either KeyHub itself or in the connected identity provider or HR-system.
2-FACTOR AUTHENTICATION (2FA)

Topicus KeyHub enforces 2FA for every user. Topicus KeyHub uses the industry standard TOTP-protocol, supported by every 2FA-app (e.g. the Google Authenticator-app, the Microsoft Authenticator-app or the Topicus KeyHub-app).

In addition Topicus KeyHub provides the possibility of connecting external 2FA-solutions. In this case Topicus KeyHub is not responsible for enforcing 2FA, but instead the external party. Organisations may consider this option when there is already a 2FA-solution in place.

SECURITY AND SESSIONS

A Topicus KeyHub-session is both IP- and browser-bound. As a result, anyone who switches IP-address or browser is required to re-authenticate via username, password and 2FA-code. Furthermore, password validation occurs every 4 hours and the 2FA-code every week.

JUST-IN-TIME PROVISIONING FOR NEW EMPLOYEES

Topicus KeyHub offers ‘just-in-time’ provisioning for new employees. If a new employee has been added to an identity provider such as a HR-system, the employee can register their own account in Topicus KeyHub. During this registration Topicus KeyHub validates this new employee against the identity provider and creates an account in Topicus KeyHub. The new employee can then be assigned a set of default groups, and individually request access to (additional) groups. This process does not require any intervention from an IT-department.
DECENTRALIZED AUTHORIZATION

All access to systems, servers, applications and shared passwords is distributed to custom groups. A group contains access to any combination of servers, systems, applications and/or a password vault. Each group has a set of group managers responsible for group memberships. Group managers are in control of all their memberships (and by extension whether a user has access to that group's specific applications and vault). Joining or leaving a group can be initiated by either a group manager or a user, and does not require the IT-department.

As a group manager can be anyone regardless of function, this means that for example:

- A product owner can be responsible for which employees are allowed access to his/her product
- A sales manager can be responsible for which colleagues are allowed access to the CRM system
- The marketing manager can be responsible for who has access to a shared social media password
- The IT-department can get back to what they do best: work on IT architecture and systems
3-LEVELS OF SECURITY

As previously mentioned, a group grants access to any combination of systems, servers, applications and a password vault. This access is divided into three possibilities, each with a different level of security.

Single Sign-on

The highest level of security is Single Sign-On (SSO). Here, no passwords exist on the Service Provider and logging on is possible only after authentication from Topicus KeyHub.

Topicus KeyHub supports various protocols including SAML2, OAuth1.0 and OAuth2.0 / OpenIDConnect. Depending on the service provider, additional features such as just-in-time provisioning may be possible. Topicus KeyHub supports user agreement as well, meaning that the Topicus KeyHub-user explicitly allows the usage of certain Topicus KeyHub-data on the connected application.

With Topicus KeyHub every Single Sign-On connection is based on a group. This means that once a user is member of a group with a SSO-connection, this user is automatically able to use that specific SSO. Once a user is removed from the group, the SSO-option is automatically withdrawn.
Real-time provisioning

The second level of access is real-time provisioning. Topicus KeyHub can connect to multiple Active Directories and/or LDAP-based systems and provide real-time provisioning of accounts on these systems. A group in Topicus KeyHub can be assigned any number of connections. After activation of a group, an account is created (LDAP) or enabled (AD). This account on the connected system can be used to log in. After deactivation of a group, the accounts are no longer available as they are either deleted (LDAP) or deactivated (AD).

For Unix-based operating systems, Topicus KeyHub allows use of an SSH-key. After enabling the specific group in Topicus KeyHub and thus creating a named account on a certain server, the SSH-key can be used to log on to that server instead of password verification.

Time-based access

The activation of a group has a default time limit of one hour. After this period Topicus KeyHub automatically deactivates the group, and the account on the server is no longer usable. Each user can decide to extend the default time period up to twelve hours. For specific groups, a group manager can decide to allow their members to extend this even further, up to two weeks.
For groups granting access to specific (high-security) systems, the reason for activation should be specified. Topicus KeyHub asks the user to provide a reason before activating the group. This reason is stored and remains visible in the audit log.

For example, a user wishes to log on to a production database for troubleshooting. Because the user is required to enter a reason for his/her wish to log on, the user becomes more aware of the potential risk associated with logging on to high-security systems.
Shared password management

When neither SSO nor real-time provisioning are possible, the last possibility is to share account credentials. Each group in Topicus KeyHub has its own password vault for storage of group-specific passwords, accounts, licences, files and other information necessary for that specific group. Every group member can access the shared password safe and add records. The Topicus KeyHub browser plugin ensures easy entry of passwords on websites etc.

Many external services have administrator accounts. These unnamed accounts provide a high risk as their credentials are often shared among multiple individuals in an organisation (these types of accounts can not easily be individualized). If such an administrator account can be configured to use 2FA, KeyHub offers the possibility to store the TOTP-secret in the vault. This means that every group member is able to generate the 2FA-code without having to share a smartphone or a hardware-token. If an employee leaves a group, logging on becomes impossible as generating the 2FA-code is no longer possible.

Personal vault

In addition to shared password vaults, Topicus KeyHub offers a personal vault as well. Employees have many personalized business accounts (e.g. for time registration systems, messenger systems like Slack). Each employee has his/her own personal password vault which can be used for all professional but individual passwords, certificates etc.

Browser extension

To enhance the user experience when entering a username / password, Topicus KeyHub offers a browser extension. With this extension, all password vault contents are easily available when needed.
A good Identity and Access Management system plays a central role in an organisation. This system should be easy to connect to any other system. Topicus KeyHub offers various possibilities to connect to other types of systems or environments, including the aforementioned OAuth 1, OAuth2 / OpenIDConnect and SAML. Other protocols and variants can be added if necessary.

### Command line interface

Topicus KeyHub comes with a Command Line Interface (CLI) with which it is possible to dynamically retrieve credentials, e.g. for use in automated scripts. Hard-coded passwords are what hackers look for, and can easily be prevented by dynamically inserting passwords via the CLI.

### Webhooks

For every action or event in Topicus KeyHub a webhook can be triggered. When a specific action (or type of action) is performed, a message is sent to a custom connected system. Whether required to send every action to a Security Information and Event System (SIEM) or to highlight the use of a specific vaultrecord on a monitor, both are possible with webhooks.

### ENCRYPTION

Topicus KeyHub uses the strongest encryption algorithms the industry offers for commercial use. Passwords in vaults are secured with multilayer AES-256 encryption using a 64k-iteration PBKDF2-SHA512 key strengthening algorithm and 4096-bit RSA keys. User passwords that are stored in KeyHub are salted and hashed using SCrypt with a high cost factor.

Furthermore, KeyHub contains a list of 500,000 widely used passwords and blocks the use of such passwords for obvious security reasons.
COMPLIANCE AND ACCOUNTABILITY

Compliance should follow from daily routine and tasks. Compliance is not something to actively pursue, but should be automatically realised in the course of normal operations. Topicus KeyHub ensures that every meaningful action a user performs is stored in an audit trail. This audit trail is easily readable for everyone (it is in a human-readable format and does not solely contain system codes and timestamps). Every step in authentication and authorization is logged, along with the specific user. Even for the use of unnamed external accounts, a user first has to log on to KeyHub to retrieve the specific password or 2FA-token. This means that even these kinds of access are accountable to the actual user involved.

With Topicus KeyHub, many of the reporting requirements for certifications like ISO 27001, NeN 7510 and SOC2 are already met.

AWARENESS CREATION

One of the biggest challenges in cyber security is creating awareness in end users. We as human beings remain the least reliable factor in security. With Topicus KeyHub all employees are bound to the same system. The ease-of-use ensures that additional security comes at low cost. With the right security layers in place, awareness increases as users are only required to perform additional actions when the risk-factor increases. Furthermore, because regaining access rights is easy, the barrier of withdrawing access rights is very low. This leads to users pro-actively withdrawing access on their own, which in turn additionally reduces risks.
Topicus KeyHub is developed in Java and runs on WildFly, building on well accomplished standards such as EJB3 and JPA.

Topicus KeyHub is not delivered as software-as-a-service but runs locally within your organisation’s infrastructure. This means your passwords and other valuable data will not be stored on any other cloud environments other than the ones under your control.

Our pre-packaged Docker containers ensure that your KeyHub installation will always be up to date with the latest security updates and features.

To conclude, code and security audits are performed periodically to ensure the highest quality and security.

The complete KeyHub-architecture: