DoubleClue White Paper

1. Introduction

The Identity & Access Management (IAM) Software *DoubleClue* facilitates the administration of identities as well as the management of access rights for various applications, systems and networks. A Multi-Factor Authentication (MFA) with eight different authentication methods is the key element of this IAM solution. Furthermore, DoubleClue has an integrated CloudSafe storage and a PasswareSafe utility, which manages user passwords based on KeePass.

2. On-Premises or Hosted in the DoubleClue.online Cloud

DoubleClue can be installed on premises and still use the default DoubleClue App from the Google Play Store or App Store. You may also host your DoubleClue Cluster in the DoubleClue.online cloud – the set up takes only a couple of minutes.

3. Multi-Tenants (Multi-Client Capability)

DoubleClue supports multi-tenants. Tenants can be defined in the DoubleClue Enterprise Management (DCEM), the central administration tool of the DoubleClue software:

- Use ONE installation, ONE database, ONE URL access for several companies or subcontractors (tenants).
- Each tenant uses an isolated database schema.
- Each tenant can administrate their users, devices, policies, LDAP, RADIUS, SAML etc. completely independently from the other tenants.
- One central point of administration manages all PKI, URLs, ports, cluster nodes and diagnostics.
- Tenants are accessible by subdomain.

DoubleClue can thus be operated as a software as a service for several clients. To use the multi-tenant capability of DoubleClue, it needs to utilize an external database. The embedded database does not support multiple tenants.

4. Access Policies

Access policies are managed in DCEM. They define with which authentication methods which users have access to applications and data.

4.1 Options

- Assignment of different authentication methods to different user groups
- Refraining of MFA within a specific time frame:
  After using MFA, users can authenticate themselves by only using their user name and password for a certain period of time.
- Browser Fingerprint:
  Calculation of a unique browser fingerprint for the distinct identification of a used browser / device. The users can authenticate themselves by username/password without MFA for a certain period if the Browser Fingerprint matches that of the previous login.
- Network Bypass:
  Define networks ranges in the Network Bypass. If a user connects from one of these network ranges, they can identify themselves by username/password without needing MFA. DoubleClue supports IPv4 and IPv6.
- Choice of Authentication Methods:
  Activate and deactivate authentication methods for different user groups. It is possible to activate several authentication methods for one user group.
- Default Authentication Method:
  Define a default authentication method for a certain user group. Users can use other authentication methods activated for their group by using a prefix before their login ID.

4.2 Assigning Policies

Access rights can be assigned to application types (e.g. RADIUS, SAML, REST-Webservices etc.) applications (e.g. Cisco Meraki, Citrix ShareFile, Dropbox etc.) and user groups.

Policy assignments are hierarchically inherited according to the following hierarchy:

a) If a user is a member of a group and this group has a policy specifically assigned to a certain application or application type, this policy is used.
b) If a user is a member of a group and this group has a general policy assigned to it, then this policy is applied if no specific policy applies for a certain application or application type.
c) If a user is a member of several groups and these groups have different assigned policies, the policy assigned to the group that has the highest priority is used.
d) If a user is a member of a group, but this group has no assigned policies, or if the user is no group member, the policy assigned to the respective application is used.
e) If an application has no assigned policy, the policy assigned to the application type is used.
f) If an application type has no assigned policy, the “Global Policy” is applied.

4.3 Global Policy

If no policy has been assigned to an application or a user group as described above, DCEM will use the “Global Policy”. The “Global Policy” is automatically created with default settings during the DoubleClue installation. After the installation, the Global Policy can be customized in DCEM, but it cannot be deleted. In a multi-tenant scenario, each tenant possesses its own global policy.

5. Authentication Methods

DoubleClue supports currently eight different authentication methods, allowing administrators and users to choose the method most suitable for their situation and preferences. Further authentication methods will be added in the future.

5.1 Push Approval

Push Approval is the most secure authentication method of DoubleClue. It is based on a PKI Private Key 2048 Bit certificate. Users receive a push notification on their smartphone. After they have logged into their DoubleClue App, they can confirm or reject the received messages and transactions. Push approval uses HTML-formatted and pre-configured templates with placeholders.
Responses are digitally signed and verified by the DoubleClue Enterprise Management.

5.2 QR-Code Approval

This one-click authentication method is based on a PKI Private Key 2048 Bit certificate and a random AES-256 encryption algorithm. Users scan a QR code with their DoubleClue App. The QR code key is usually valid for two minutes.

5.3 FIDO U2F and FIDO2 Token

FIDO is an open standard for multi-factor authentication. FIDO Security Keys are physical tokens that connect to a device via the Bluetooth or USB interface. FIDO2 implements biometric identification via fingerprint for further security. For more information, visit https://fidoalliance.org/.

5.4 OTP Token

OTP tokens are hardware tokens generating a one-time password for every login. The user enters the one-time password in addition to their user password. DoubleClue supports the token type "**TIME_6_SHA1_60**". This is a time-based OTP with 6 digits using an SHA1 algorithm and a time slot of 60 seconds.

5.5 DoubleClue Passcode

Users can generate an offline passcode with their DoubleClue App if no internet connection is available.

5.6 Password

A user logs in with user name and password only. This classic identification method is intended for applications in certain trusted networks for which an MFA is not essential.

5.7 SMS

A random passcode is created and sent to the user's mobile phone via SMS. The SMS Passcode is transmitted without any encryption! This method is normally used in addition to the login with password.

5.8 Voice Message

A random passcode is created and sent to the user by a call to their landline or mobile phone. The Passcode is transmitted without any encryption!

6. DoubleClue App

6.1 Universal DoubleClue App

The default DoubleClue App is provided for Android, iOS, Windows Desktop, MAC and Linux. It can be downloaded from Google Play Store or App Store. Please contact support@doubleclue.com for other operating systems.

After the installation, the App is activated by entering the username, password and an activation code. User-name and activation code can be automatically inserted via QR Code scan. During the activation process, a Private Key is generated. The Private Key does not leave the smart device and is stored on it in encrypted form. It is necessary to digitally sign message transactions.

As DoubleClue identifies the unique DNA of smart devices upon installation, the activated app only functions on the respective device. It can't be cloned on another device.

Users can install and activate their DoubleClue App on different platforms. An App installed and activated on one device supports usage by several different users.

App requirements:

- Android: Version 5.0 (Android Lollipop) or newer
- Windows: Version 7, 8, 10
- iOS: Version 10.0 or newer

6.2 DoubleClue SDK-Library for Android and iOS

The DoubleClue App consists of a DoubleClue SDK library and the App GUI. With the help of the SDK library, the DoubleClue features can be integrated into one's own company app, or a customized DoubleClue App can be created.

7. Integration of Applications with DoubleClue

DoubleClue supports third party applications via the following interfaces:

- REST Web-Services
- RADIUS
- SAML
- OpenID-OAuth
- Auth-Connector (for example for Windows Login)
- RD Web Access (via plugin)
- ADFS Plugin
- Windows Login Credential Provider

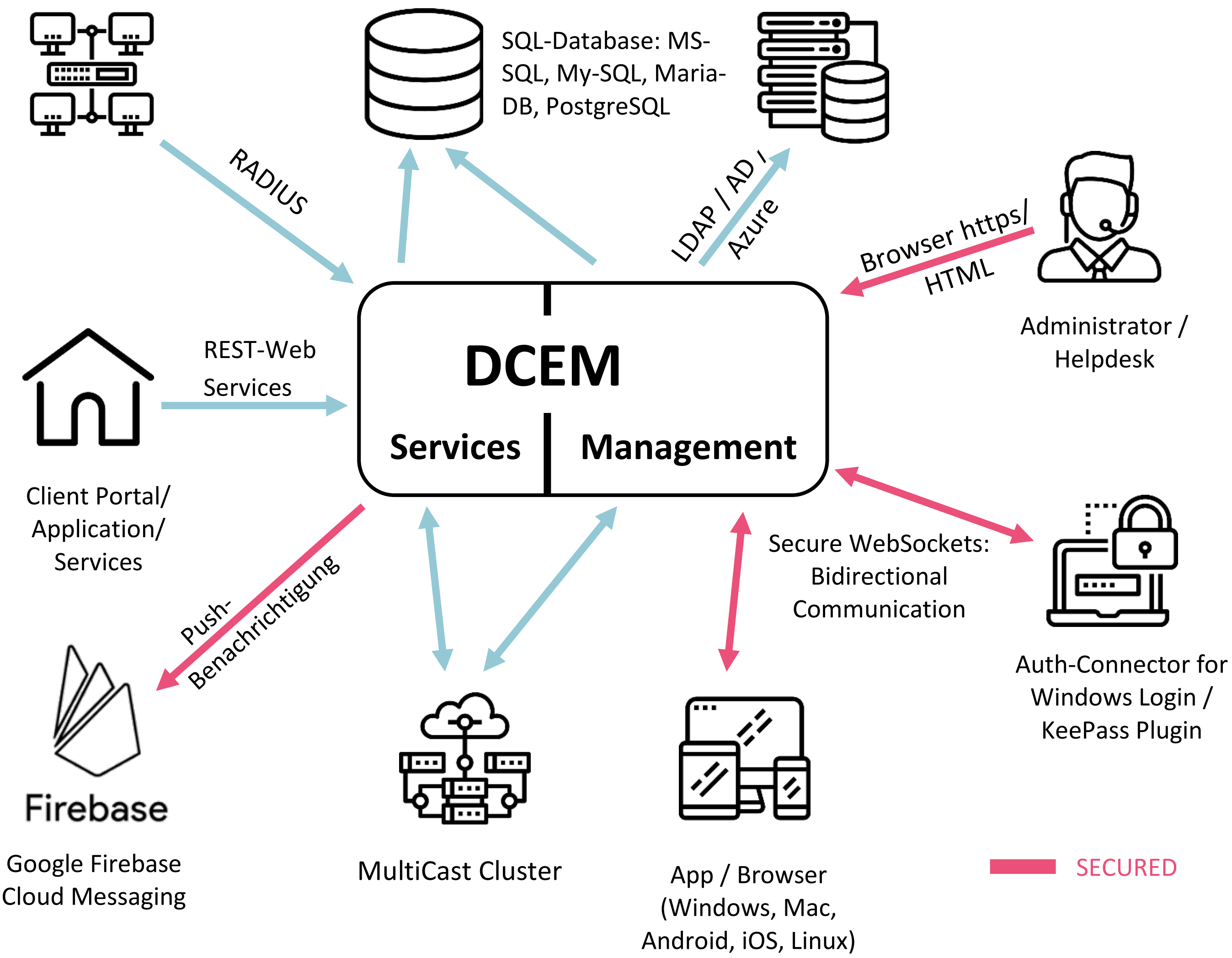
8. DoubleClue Enterprise Management (DCEM)

8.1 Feature Overview

- Single point of administration for users, devices, administrators, access policies, tenants etc.
- DoubleClue Enterprise Management can be installed on premises or it can be hosted on doubleclue.online
- High fail-safety due to load distribution by highly scalable cluster nodes. The necessary load balancer is not part of the DoubleClue solution.
- Finely tuned, role-based access rights for administrators
- History about every change
- Integration of and communication with company applications via the interfaces listed above
- Communication with the DoubleClue App via secure Web Sockets
- Usage of an own PKI for communicating with the DoubleClue App. Thus, the App is independent from the operating system’s PKI.
- Own built-in Certificate Authority with support for external CAs
- Support of an integrated database (“Embedded Database”) as well as the external databases Maria DB, MySQL, MS SQL and PostgreSQL
- Runs on Windows and Linux
- Full Active Directory integration (domains, users and groups from Active Directory, Azure AD and LDAP)
- Supports multiple-domain infrastructure

8.2 Structure of DCEM

DCEM is a cluster that consists of several interlinked independent servers. It is the central component of the DoubleClue platform.
DCEM is divided into several areas. The following scenario demonstrates all possible components of DCEM and the areas with which they communicate:

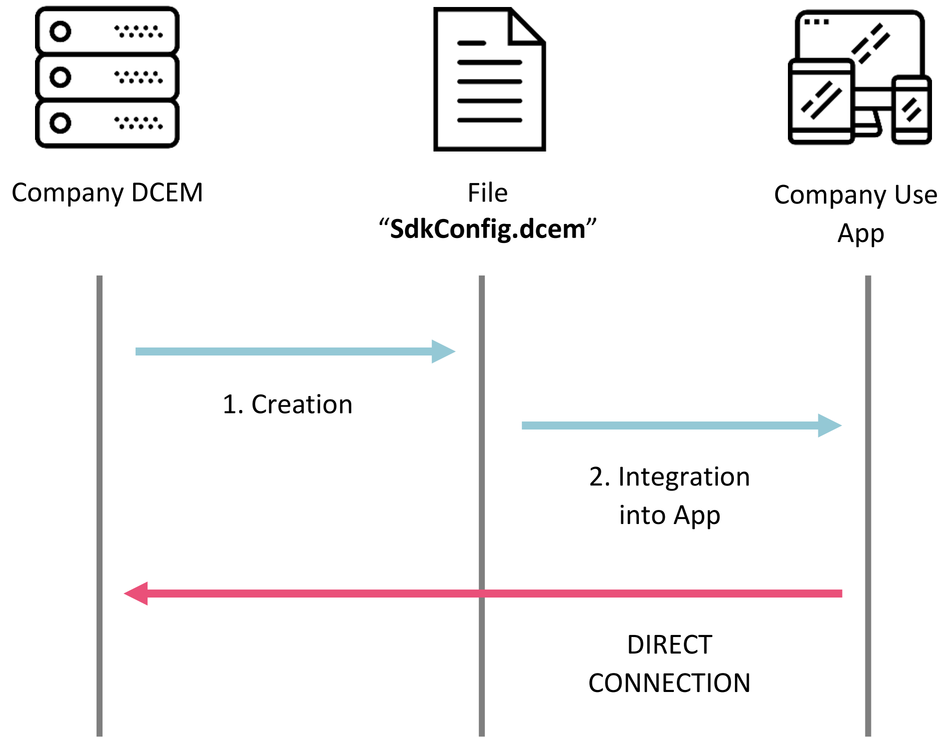

SQL-Database: MS-SQL, My-SQL, Maria-DB, PostgreSQL
RADIUS
LDAP / AD / Azure
Browser https/ HTML
Administrator / Helpdesk
REST-Web Services
DCEM
Services
Management
Client Portal/ Application/ Services
Secure WebSockets: Bidirectional Communication
Push-Benachrichtigung
Auth-Connector for Windows Login / KeePass Plugin
Firebase
Google Firebase Cloud Messaging
MultiCast Cluster
App / Browser (Windows, Mac, Android, iOS, Linux)
SECURED

8.3 Connection Scenarios

The DoubleClue App can connect to DCEM directly or via the global DoubleClue Dispatcher.

8.3.1 Direct Connection with In-House App

The App directly connects to a company's DCEM installation. For this connection type, customers need to create their own app and integrate the DCEM certificates into it.



8.3.2 Connection via the DoucbleClue Dispatcher

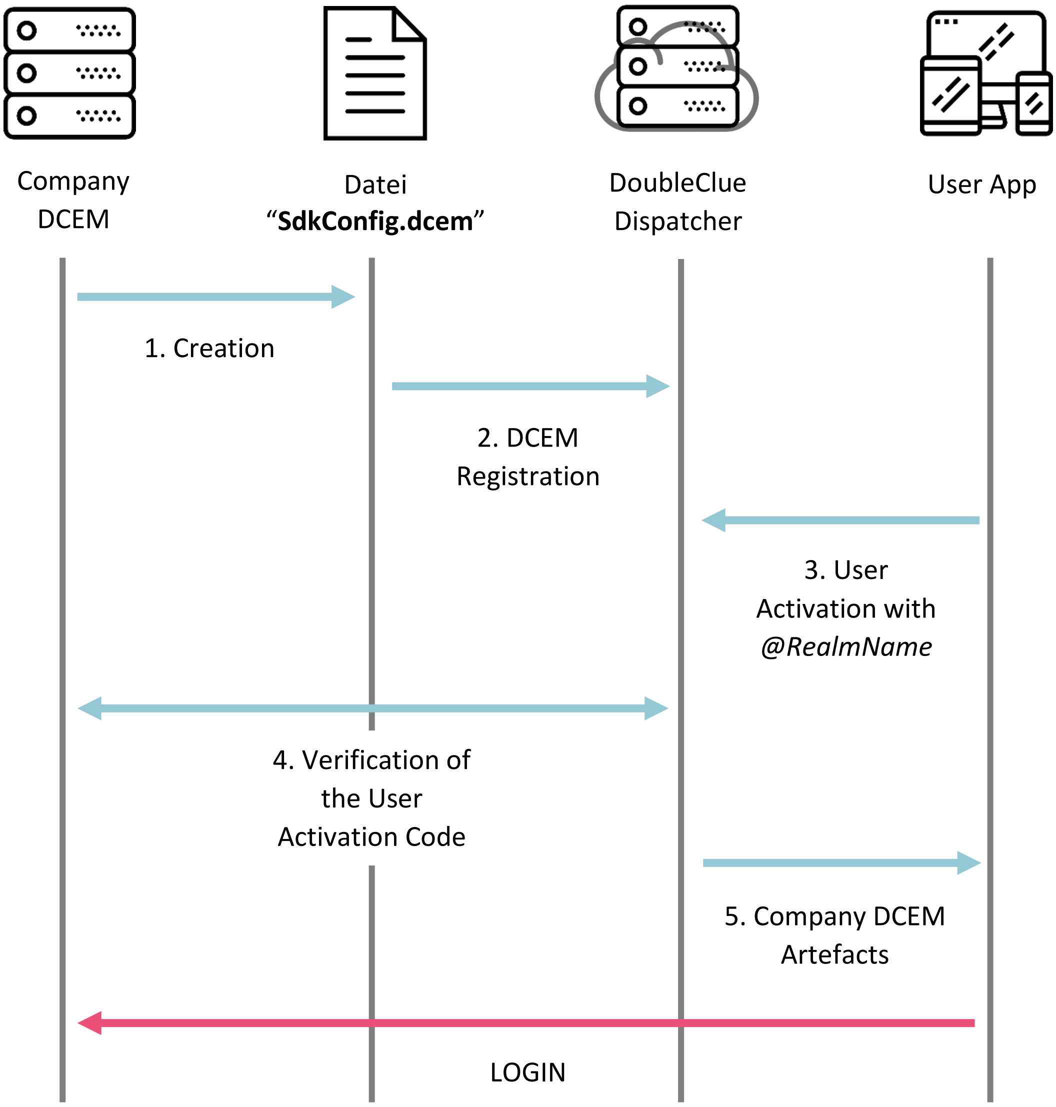
This connection type allows the usage of the universal DoubleClue App. It needs the installed DCEM to be registered at the global DoubleClue Dispatcher.

⚠ Requirement: DCEM port 443 must be accessible from the internet. Please change your firewall settings.

Prerequisites are that the DCEM cluster has a Domain Name System (DNS) and the secure Web Sockets port is open for the internet.

The DoubleClue Dispatcher is a DCEM Cluster in the cloud managed by *HWS Informationssysteme GmbH*. On device activation, the Dispatcher will verify login ID and activation code with the domain

"Dcem-Installation". If the Activation Code is valid, the Dispatcher will send the DCEM SDK configuration metadata file to the device. At login, the device will connect directly to a company's DCEM installation.


Company DCEM
Datei "**SdkConfig.dcem**"
DoubleClue Dispatcher
User App
1. Creation
2. DCEM Registration
3. User Activation with *@RealmName*
4. Verification of the User Activation Code
5. Company DCEM Artefacts
LOGIN

8.3.3 Connection to the DoubleClue Dispatcher via Reverse-Proxy

For testing purposes, you can establish a connection through the DoubleClue Dispatcher via Reverse-Proxy. In this scenario, your DCEM will connect to the DoubleClue Reverse-Proxy and all data goes through a tunnel between your DCEM and DoubleClue Reverse-Proxy. Therefore, you do not need to open a listening port on your firewall.

8.4 User Roles

Users can be assigned one of several roles that can be fully customized or newly added by the DoubleClue administrators. Roles can be individualized for each tenant and range from simple users that can't access DCEM at all, to different ranks of administrators for certain connection services or the whole DoubleClue Infrastructure. Different user roles can be specified for each tenant.

9. UserFeatures

9.1 UserPortal

DoubleClue UserPortal is a self-service portal for DoubleClue users. It allows the users to register themselves and manage the smart devices, FIDO tokens and OTP tokens connected with their DoubleClue account without the help of an administrator. It also gives access to PasswordSafe and CloudSafe.

The different sections and actions available in the UserPortal are fully customizable by the administrators. It is further possible to specify two different kinds of access: a restricted access if users log in only using their passwords and a wider access if they log in with MFA.

9.2 PasswordSafe

DoubleClue PasswordSafe is a password manager allowing to store user passwords in the DoubleClue infrastructure. It secures the passwords with the DoubleClue multi-factor authentication, while ensuring that they are easily accessible for the users at the same time. The passwords can be managed via the DoubleClue Apps or by using UserPortal Web UI. Password files are never stored locally on a device or workstation. The PasswordSafe files format is compatible with KeePass.

9.2.1 KeePass Plugin

The DoubleClue KeePass Plugin allows the easy upload or download of PasswordSafe files to and from a windows desktop computer. It is compatible with KeePass Password Safe 2.4.0 and higher.

9.3 CloudSafe

DoubleClue CloudSafe is a cloud storage for important and confidential files and documents. It is accessible through DoubleClue UserPortal. Files in CloudSafe are secured by the DoubleClue MFA and an AES encryption. DoubleClue users can share their files with other users of the same tenant.

It is further possible to save the single files with an additional password. This adds another layer of encryption with salts to the file.