# DoubleClue Whitepaper

*Version 1.5.1 von 20. Okt. 2018*

## 1. Einleitung

Die Identity & Access Management (IAM)-Software *DoubleClue* ermöglicht die Administration von Identitäten sowie die Verwaltung von Zugriffsrechten für verschiedene Applikationen, Systeme und Netzwerke. Eine Multi-Faktor-Authentifizierung mit sieben verschiedenen Authentifizierungsmethoden ist dabei ein wesentlicher Bestandteil der IAM-Lösung.

## 2. Access Policies

Im DoubleClue Enterprise Management können zentralisierte „Access Policies“ eingerichtet werden. Damit kann definiert werden, welche Benutzer mittels welcher/welchen Authentifizierungsmethode/n auf welche Applikation/en zugreifen dürfen.

Zugriffsrechte können Benutzergruppen, Applikationstypen wie SAML und RADIUS sowie individuellen Applikationen zugewiesen werden.

Bei Bedarf kann der Benutzer selbst aus den vorkonfigurierten Authentifizierungsmethoden wählen.

## 3. Authentifizierungsmethoden

Ausgehend von einer Cluster-Farm als einzigem, zentralisiertem Verwaltungspunkt werden Benutzer von DoubleClue für verschiedene Applikationen authentifiziert. Benutzer haben dabei die Option, aus mehreren Authentifizierungsmethoden zu wählen.

### 3.1 Password

Ein Benutzer meldet sich nur mit Benutzername und Passwort an. Diese klassische Variante ist für Applikationen aus bestimmten vertraulichen Netzwerken gedacht, für deren Nutzung eine MFA nicht zwingend notwendig ist.

### 3.2 SMS Passcode

Zusätzlich zur Authentifizierung mit Passwort wird ein zufälliger Passcode erstellt, der per SMS an das Mobiltelefon des Benutzers gesendet wird. Der SMS- Passcode wird dabei unverschlüsselt übertragen!

### 3.3 Voice Message

Zusätzlich zur Authentifizierung mit Passwort wird ein zufällig generierter Passcode per Anruf auf dem Festnetz- oder Mobiltelefon eines Benutzers durchgegeben.

### 3.4 Hardware Token

Zusätzlich zur Authentifizierung mit Passwort geben Benutzer ihr Passwort ein und der One-Time Passcode (OTP) wird vom Hardware Token generiert.

### 3.5 DC App Passcode

Falls keine Internetverbindung verfügbar sein sollte, generieren Benutzer mit Hilfe ihrer DoubleClue-App einen Offline-Passcode.

### 3.6 DC Secure Message

Die sicherste Authentifizierungsmethode basiert auf einem PKI Private Key 2048 Bit-Zertifikat. Benutzer erhalten eine Push-Benachrichtigung auf ihrem Smartphone. Nachdem sie sich in ihre DoubleClue-App eingeloggt haben, können sie sichere Meldungen und Transaktionen bestätigen oder ablehnen.

Die Meldungen sind HTML-formatiert und als Template mit Platzhaltern vorkonfiguriert.

Rückmeldungen werden digital signiert und beim DoubleClue Enterprise Management verifiziert.

### 3.7 Secure QR Code

Die One-Click-Authentifizierungsmethode basiert auf einem PKI Private Key 2048 Bit-Zertifikat und einem AES-256 zufälligen Verschlüsselungsalgorithmus. Benutzer scannen mit Hilfe ihrer DoubleClue-App einen QR-Code. Der QR-Code-Schlüssel ist in der Regel nur für zwei Minuten gültig.

## 4. DoubleClue-App

### 4.1 Universelle DoubleClue-App

Die Standard-DoubleClue-App steht für Android, iOS, Windows Desktop, MAC und Linux zur Verfügung. Sie kann direkt vom Google Playstore oder vom App Store heruntergeladen werden. Für andere Betriebssysteme kontaktieren Sie bitte support@doubleclue.com.

Nach der Installation wird die App mittels Benutzername, Passwort und einem Aktivierungscode aktiviert. Bei diesem Prozess wird ein Private Public Key erstellt. Der Private Key verlässt das smarte

Gerät nicht und wird in verschlüsselter Form darauf gespeichert. Er wird benötigt, um Meldungs-Transaktionen digital zu signieren.

Da DoubleClue die einzigartige DNA von smarten Geräten identifiziert, funktioniert die aktivierte App nur auf dem entsprechenden Gerät.

Benutzer können die DoubleClue-App auf verschiedenen Plattformen installieren und aktivieren.

Eine auf einem Gerät installierte und aktivierte App unterstützt auch die Nutzung durch mehrere verschiedene Benutzer.

App-Anforderungen:

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

### 4.2 DoubleClue SDK-Library für Android und iOS

Die DoubleClue-App besteht aus einer DoubleClue SDK-Library und der App-GUI. Mit Hilfe der SDK-Library kann die DoubleClue-Funktionalität in die eigene Unternehmens-App integriert werden, oder es kann eine auf das jeweilige Unternehmen zugeschnittene DoubleClue-App erstellt werden.

## 5. Anbindung von Applikationen an DoubleClue

DoubleClue unterstützt alle Applikationen über folgende Schnittstellen:

- REST-API Services
- RADIUS
- SAML

## 6. DoubleClue Enterprise Management (DCEM)

### 6.1 Features im Überblick

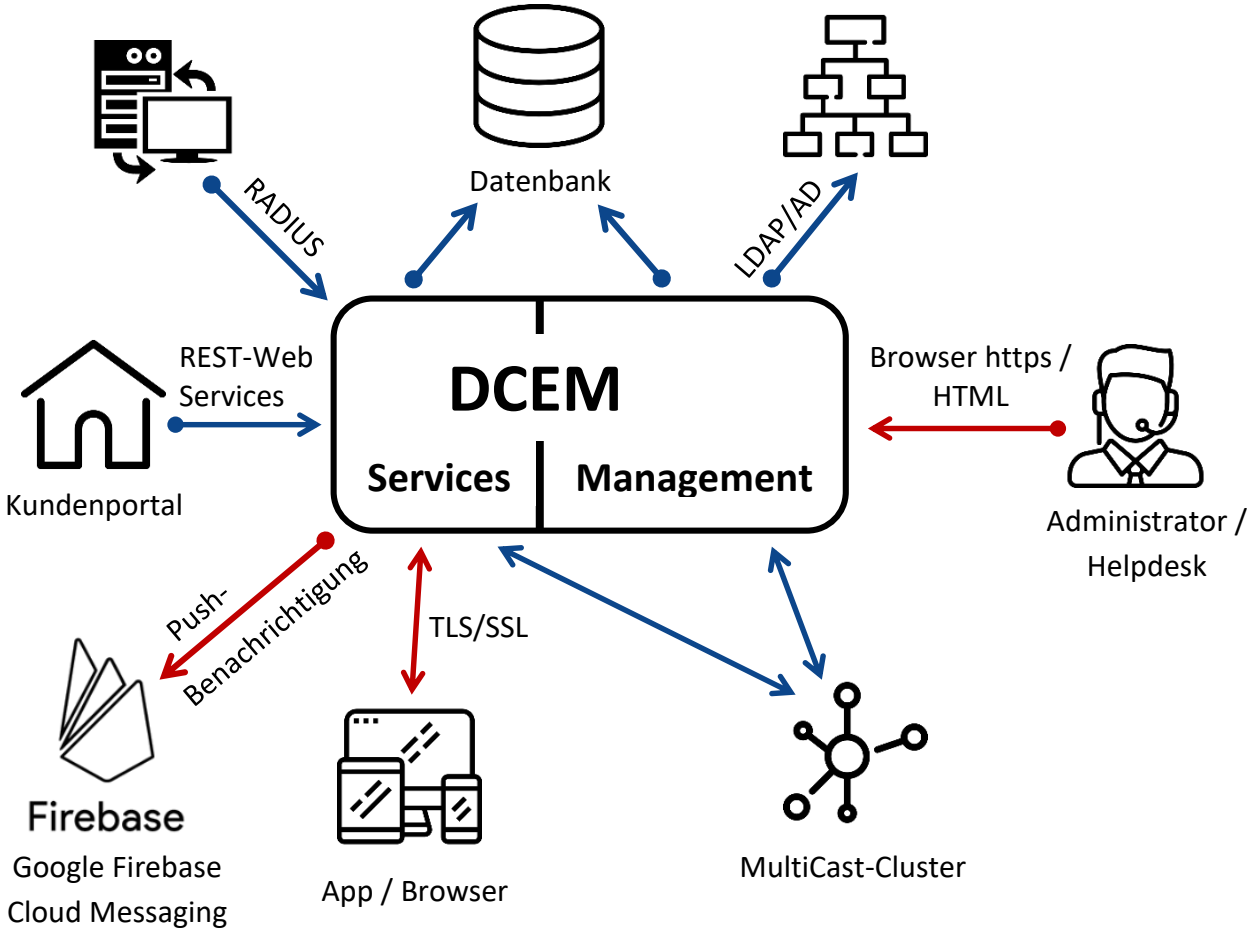
- Single Point of Administration für Benutzer, Geräte, Operatoren, Access Policies etc.
- Hohe Ausfallsicherheit durch Lastenverteilung mittels hochskalierbarer Clusterknoten. Der benötigte Load-Balancer ist nicht Teil der DoubleClue-Lösung.
- Fein abgestimmte, rollenbasierte Zugriffsrechte für Operatoren
- Historie über jede Änderung
- Integration und Kommunikation mit Unternehmensapplikationen per REST Web-Services, RADIUS oder SAML
- Kommunikation mit der DoubleClue App über Secure Web Sockets

- Verwendung einer eigenen PKI für die Kommunikation mit der DoubleClue-App. Die App ist damit unabhängig von der PKI des Betriebssystems.
- Eigene eingebaute Certificate Authority mit Unterstützung für externe CAs
- Unterstützung einer integrierten Datenbank („Embedded Database“) sowie der externen Datenbanken Maria DB, MySQL und MS SQL
- Für Windows und Linux
- Volle Integration des Active Directory (Domains, Benutzer und Gruppen)
- Bereit für Multiple-Domain-Infrastruktur
- Unterstützung von Cloud-Daten für Geräte und Benutzer

## 6.2 Aufbau von DCEM

DCEM ist ein Cluster, welches aus mehreren miteinander vernetzten, eigenständigen Servern besteht. Es ist die zentrale Komponente der DoubleClue-Plattform.

DCEM ist in die Bereiche „Management“ und „Services“ getrennt. Dieses Szenario stellt alle möglichen Komponenten von DCEM dar und mit welchem Bereich sie kommunizieren:

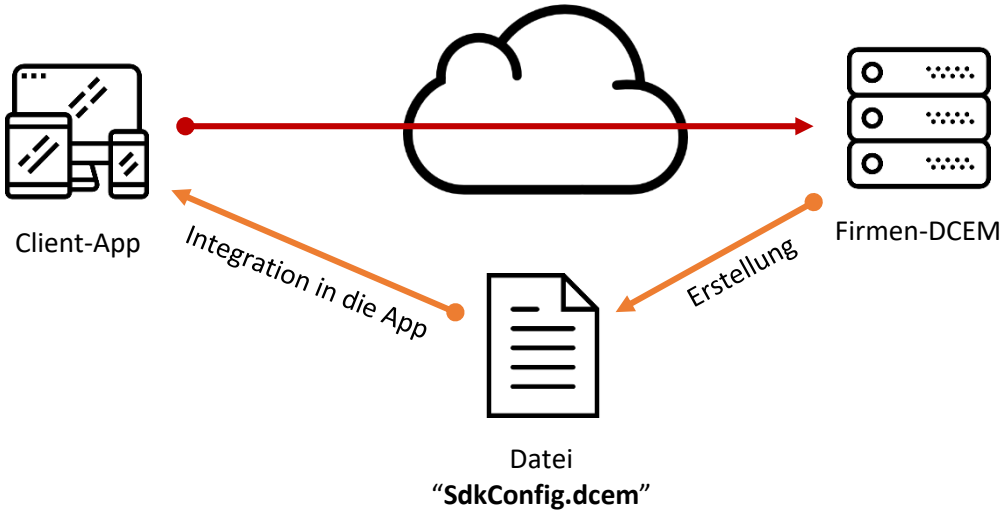



## 6.3 Verbindungsszenarien

Die DoubleClue-App kann sich direkt oder über den globalen DoubleClue-Dispatcher mit DCEM verbinden.

### 6.3.1 Direkte Verbindung

Die App verbindet sich direkt mit der Firmeninstallation von DCEM. Bei diesem Verbindungstyp muss der Kunde seine eigene App erstellen, da die DCEM-Zertifikate in die kundenspezifische App integriert sein müssen.



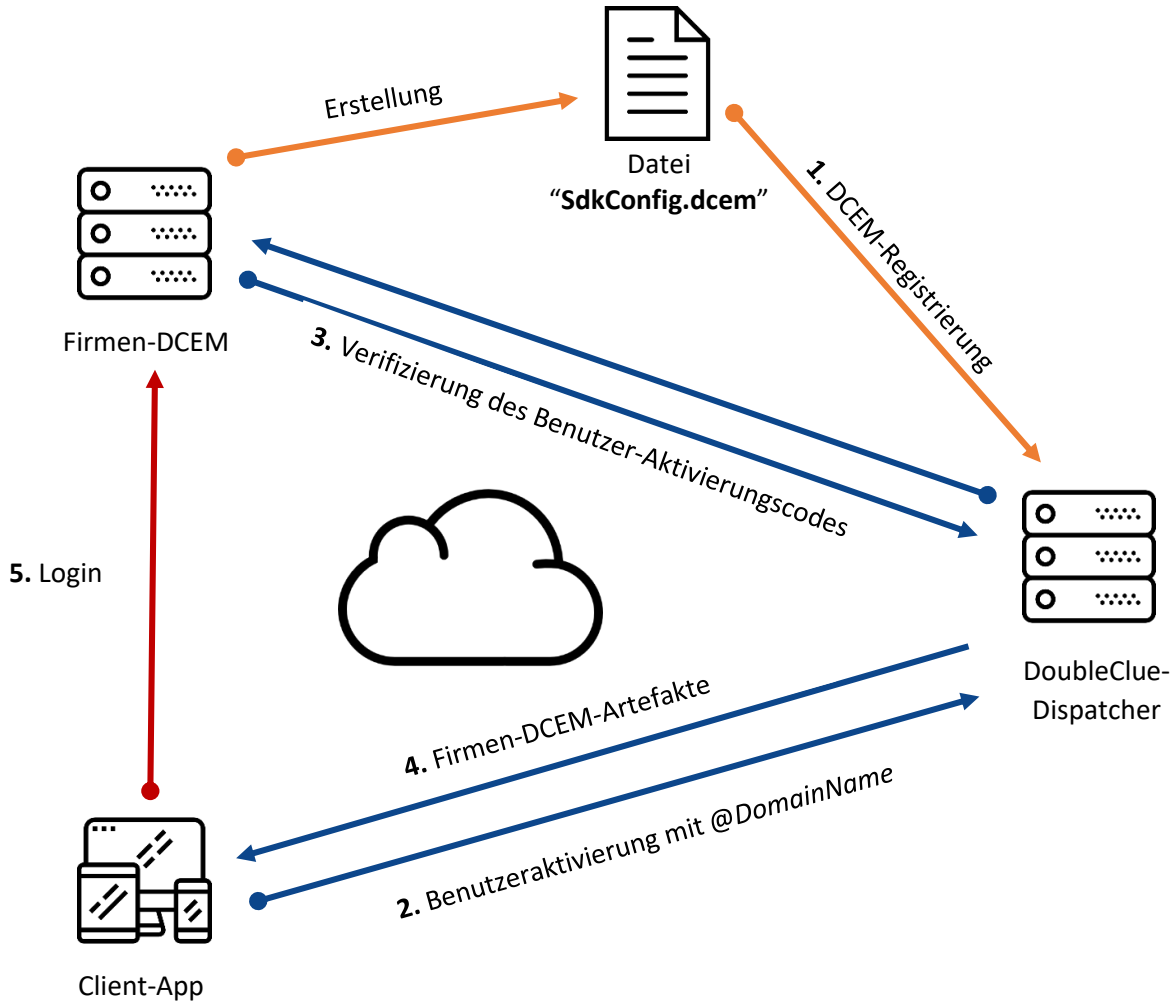

### 6.3.2 Verbindung über den DoubleClue-Dispatcher

Bei diesem Verbindungstyp kann die universelle DoubleClue-App verwendet werden. Dabei muss das installierte DCEM-Cluster zuvor beim globalen DoubleClue-Dispatcher registriert werden.

Voraussetzung dafür ist, dass das DCEM-Cluster ein Domain Name System (DNS) hat und der Secure Web Sockets-Port für das Internet geöffnet ist.

Der DoubleClue-Dispatcher ist ein DCEM-Cluster in der Cloud, die von der *HWS Informationssysteme GmbH* verwaltet wird. Bei der Geräteaktivierung verifiziert der Dispatcher Benutzer-Anmeldename und Aktivierungscode mit der Domain “Dcem-Installation”.

Ist der Aktivierungscode gültig, sendet der Dispatcher die DCEM-SDK-Konfigurationsdatei zu dem Gerät. Bei der Anmeldung verbindet sich das Gerät direkt mit der Firmeninstallation von DCEM.


Erstellung
Datei
"SdkConfig.dcem"
1. DCEM-Registrierung
Firmen-DCEM
3. Verifizierung des Benutzer-Aktivierungscodes
5. Login
DoubleClue-
Dispatcher
4. Firmen-DCEM-Artefakte
2. Benutzeraktivierung mit @DomainName
Client-App