Whitepaper: Security architecture of Ceetron Cloud and building security into Ceetron Cloud Private

ceetron®
understanding by visualization

Whitepaper for external distribution

Prepared by Fredrik Viken, CTO

Abstract

Ceetron Cloud is a web platform for sharing and collaboration on CAE models. It has been designed with security as a primary focus, while still making it easy to use and access.

Ceetron Cloud runs on Microsoft Azure and utilizes the built-in security offered by Azure. The services allow users full control of how their models are shared using four levels of security: Public, sharable (via link), group (login required) and private (only accessible for the owner of the model).

Customers who want to have their own 'Ceetron Cloud' have two options: Run a copy of it on their own cloud provider of choice (not limited to Azure) or run it on premises on own hardware behind the company firewall (Ceetron Cloud Private). In both cases the customer has full control and access to all data, whereas Ceetron cannot access any part of the service (not even usage logging/telemetry or licenses checks).

Ceetron Cloud Private offers the most protection, as the entire service is run behind the company firewall. This does limit the ability to share models with external users (as they can access the service via a VPN, for example), but offers the maximum security.

Revision history

Version	Date	Author	Status	Description
1.0	24.09.2018	FV	Initial version	First release of document
0.9	14.08.2018	FV	Work in progress	This is the first version of the document

Contents

1 Purpose of this document

The intended reader of this document is an IT professional with responsibility for IT infrastructure for CAE computing and storage infrastructure.

The purpose of this document is twofold:

1. To describe the security architecture of Ceetron Cloud.
2. To discuss the security architecture of Ceetron Cloud Private, using Ceetron Cloud as a reference architecture, assuming that the reader will want to extend and / or replace components of Ceetron Cloud.

Ceetron makes no claim as to the level of security of this architecture. The reader is encouraged to make an independent assessment of the security level of Ceetron Cloud and Ceetron Cloud Private. Ceetron is not in the position to provide services in this area.

2 The security challenge in cloud-based CAE

The transition from on premise computer infrastructures to off-site cloud-based infrastructures has created a lot of questions and uncertainties related to security. Security in a cloud-based service architecture is complex and it is truly a big challenge to assess the overall security of a given application or service hosted on public cloud infrastructures. Or private cloud for that matter. Whether an automotive manufacturer designing a new super-cool high-performance premium car model, an engineering specialist consultancy with a need to protect confidentiality of client material, or a software provider in SPDM space with a business imperative of guaranteeing the security of their cloud solutions to their blue-chip aerospace clients, protecting CAE data against intentional or unintentional release to an untrusted environment is imperative.

In this whitepaper, we will describe how Ceetron has designed and implemented different levels of security around data being stored on Ceetron Cloud. The whitepaper also discusses how Ceetron Cloud can be integrated into existing cloud-based service architectures allowing an organization to completely control the security around the data stored on Ceetron Cloud.

3 Public cloud vs. private cloud

Ceetron offers three approaches to cloud-based storage/viewing:

- **Ceetron Cloud.** Smaller companies who just want a quick and easy way of enabling sharing in their applications should in most cases be happy with Ceetron Cloud. Other customers, say OEMs or large end users, may for various reasons require a branded version of Ceetron Cloud.
- **Branded Ceetron Cloud.** A branded/skinned version of Ceetron Cloud running on a cloud provider of choice (AWS/Azure/IBM/internal data center/etc.) or on on-premises hardware exposed to the internet. It could use a custom user

authentication scheme (see below), but is exposed to the internet and secured in the same way as Ceetron Cloud.

- **Ceetron Cloud Private.** This is integration of web-based visualization and progressive 3D object streaming of CAE data into an existing private cloud infrastructure behind the company firewall. In this scenario, the customer would take care of all aspects of security. Users would need to have access to the internal network (on premises or via VPN) to even reach the Ceetron Cloud Private Web Application.

4 Security architecture of Ceetron Cloud

4.1 Built on secure technology

Ceetron Cloud is hosted on MS Azure.

All communication between the client and server uses SSL (https) with an EV Certificate with Extended Validation. To obtain security validation, several online third-party scanners is used to check cloud.ceetron.com for vulnerabilities.

Ceetron Cloud uses MS AD B2C identity management for user authentication together with OAuth 2.0, the industry-standard protocol for authorization. For more details, see section 5.2.

Ceetron Cloud can accommodate four standard levels of security:

- **Public:** Public models can be found through browsing or searching on Ceetron Cloud, and can be viewed by everyone.
- **Shareable:** Shareable models can be seen only by those who have the required link. The security is good, as the link is a GUID (RFC4122 v4 UUID, base64 encoded) that is virtually impossible to guess. If it were possible to make a billion guesses per second for the next hundred years, the chance of guessing correctly would still only be 50%. User must remember, however, that anyone intercepting the email/chat carrying the link can then look at the model.
- **Group**: Users can create and share models to a group. In order to view a shared model, group members must be logged in to Ceetron Cloud. Users outside the group have no access, even if they possess the model link.
- **Private:** Access is restricted to the owner of the model, who must be logged in to Ceetron Cloud. Nobody else can view the model, even if they possess the model link.

4.2 On a personal level: protect your account

It goes without saying: Security depends on individuals as well as on a solid security architecture. Which means strong and unique passwords, monitoring of account activity, and organizational discipline when sharing CAE models through links.

Users should never divulge their password to anyone, including trusted team members and admins. Users must refuse any verbal or written request for their password from anyone. We at Ceetron will never under any circumstances ask for a user's password.

Users must be diligent when opening emails or other correspondence containing links to Ceetron Cloud. Phishing attacks, where attackers target users with specially crafted emails that look legitimate but link to their own malicious sites, are a very real threat for any organization possessing sensitive data. Users must always check that the email sender has a legitimate company email address. If in doubt, users are recommended to open Ceetron Cloud manually in their browser rather than clicking on the link.

Users are recommended to enable two-factor authentication whenever possible, so that their account is still protected even if their password is compromised. two-factor authentication is only available when using external identity management (see section 5).

5 Building security into Ceetron Cloud Private

5.1 Installing Ceetron Cloud on premise

Organizations who run their own on-premise computer infrastructures and would like to offer the Ceetron Cloud data sharing service may do so by installing a private installation of Ceetron Cloud. A private installation will allow the IT department to completely control security and user access to all data stored in Ceetron Cloud. There is no way for Ceetron to access the installation or to monitor any usage of it (even for license checking).

The easiest way to get started with Ceetron Cloud Private is to use Docker. We have a ready to run setup which will get you up and running within minutes.

5.2 Customizing the user authentication

Ceetron Cloud uses an OAuth2-based authorization framework. Ceetron Cloud as public cloud uses Azure Active Directory B2C, but there is also an implementation for Auth0. Ceetron can assist customers in creating adapters for company-specific authorization schemes. CC Private also has an option to run with a simple username / hashed password scheme for easy to setup installations behind a company firewall.

Ceetron Cloud private can be configured with the following security policies:

- **External Identity Management:** Authentication is handled by an external service.
    - Currently Microsoft Azure Active Directory B2C and Auth0 are supported.
    - OAuth 2.0 is utilized, the industry-standard protocol for authorization.

    - The Ceetron Cloud SPA uses OAuth 2.0's implicit grant type, which is the recommended flow for SPAs: To log in, the user is redirected to the external identity management service's login portal. The sending and validation of user credentials happens completely outside the bounds of Ceetron Cloud. Once authenticated, the user is returned to Ceetron Cloud with an access token, which grants the user time-limited access to the Ceetron Cloud API.
    - Other applications can use the same login portal to request the user for restricted access to their Ceetron Cloud account to perform actions on their behalf. For example, in order to upload models to user accounts, Analyzer Desktop requests the user to login and grant it upload access to their account. Once granted, Analyzer Cloud is only able to upload models to the user's account. Attempts to perform any other action are blocked.
    - This is the policy used by Ceetron Cloud.
- **Local Identity Management:** A simpler solution for organizations not requiring the bells and whistles of OAuth 2.0.
    - Login occurs within the Ceetron Cloud SPA.
    - Salted hashed passwords are stored in an on-premise database.
    - Even though passwords are sent to the server in encrypted form, it is strongly recommended that communication uses https.
    - Users grant applications upload access to their accounts by providing them with their upload ID.

6 Summary

Ceetron Cloud offers a secure and simple way to share CAE models. It is built with security as a first-class citizen, and offers the maximum security option with Ceetron Cloud Private.

With the option of integrating with External Identity Management through OAuth 2.0 it is easy to utilize mature tried-and-tested services, leveraging extra features such as two-factor authentication.