

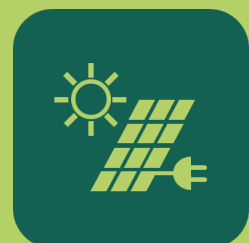
White Paper

How Will the Cloud of the Future Look Like?

- So secure that it can be sovereignly used
- Minimal greenhouse gas emissions
- Easy-to-use



BetterEdge
Verifiable Sovereign Computing



Whitepaper:
How Will the Cloud of the Future Look Like?

real-cis GmbH
Munich · Frankfurt
Rheinstr. 5, Langen 63225 GERMANY

<https://betteredge.de>

Date of creation: 17.09.25

© real-cis GmbH. All rights reserved.

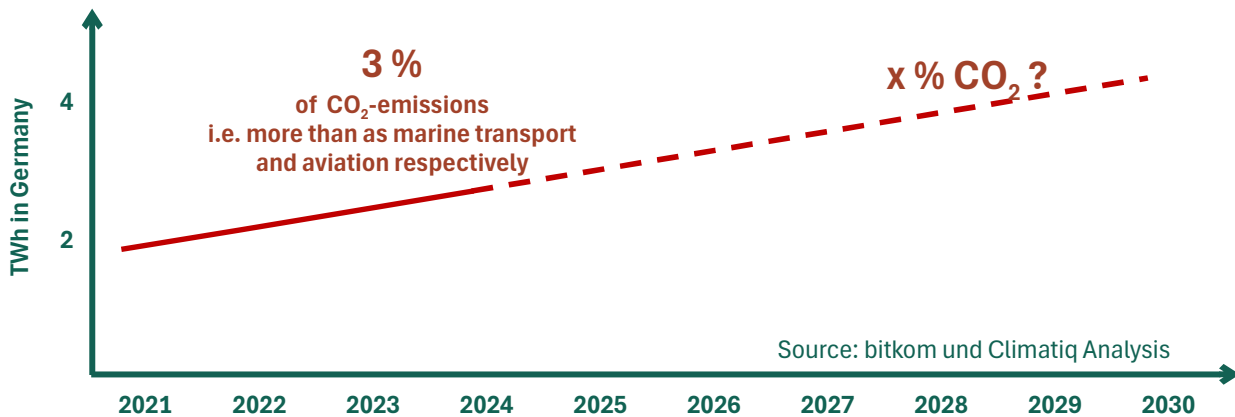
Table of Contents

1. Problems of Cloud Computing	2
1.1 Significant energy usage and CO ₂ emissions	
1.2 Missing data-sovereignty	
2. Cloud-Strategies and Demand	3
2.1 Hesitance from users & on-premises servers	
2.2 Verifiable digital sovereignty	
3. Solutions and EU-Innovation	4
3.1 Cross-sector innovation	
3.2 Open source software	
3.3 Thinking ahead of the game	
4. Distributing Servers	5
4.1 Physical access protection ensures trust	
4.2 Two types of innovative Edge Cloud Modules	
4.3 Symbiosis with Photovoltaics	
4.4 Best practice Confidential Computing	
4.5 Perfect Root of Trust	
4.6 Verifying integrity cryptographically	
4.7 Automation reduces labor cost	
5. This is the Cloud's Future	8
5.1 Less data centres, more distribution	
5.2 Everything depends on the connectivity	
5.3 Rise resilience of critical infrastructure	
5.4 Your benefits are to start today	

1. Problems of Cloud Computing

1.1 Significant energy usage and greenhouse gas emissions

Even though the amount of energy needed per computation is exponentially being reduced (due to the reduction of the size of electronics), the amount of energy that data centres need doubles within 10 years (not including processes for cryptocurrency). The generation and distribution of the electricity, combined with the production of the hardware now account for 3% of CO₂ emissions.



With the amount that IT and AI is needed for increasing efficiency, the usage of cloud-technologies is a big contributing factor to the ongoing climate catastrophe. The amount of greenhouse gas emissions due to cloud computing must be drastically reduced.

1.2 Missing Data Sovereignty

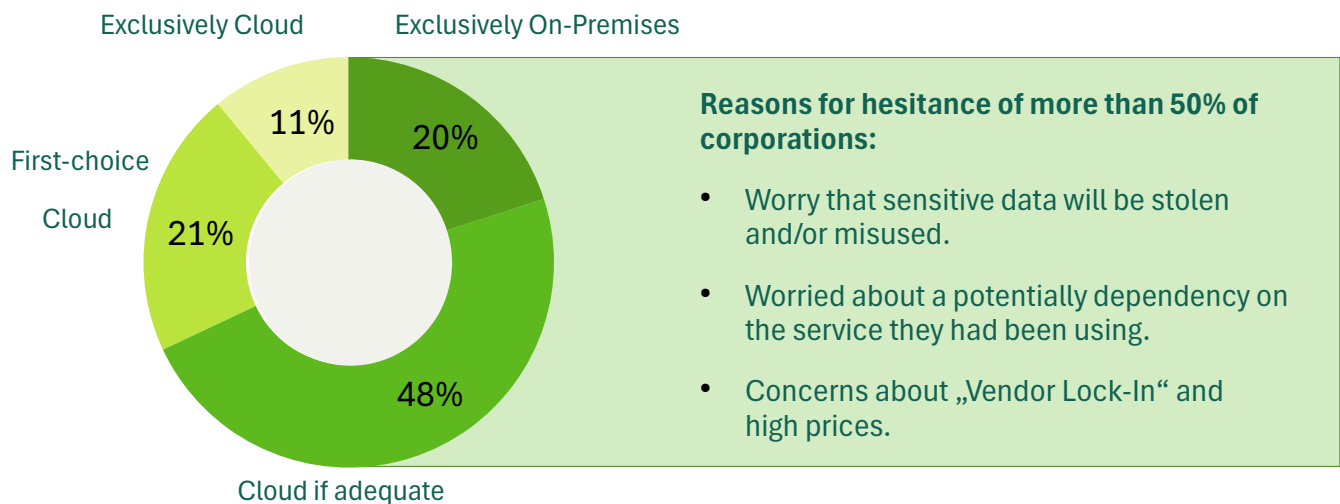
Data sovereignty does, on the one hand, not exist due to security gaps in the technology, and on the other, does not exist due to the mismatched legal systems in the USA and Europe. Cloud operators and administrators often have unnecessarily privileged access to their users' data and code – not because they are particularly trustworthy, but because conventional technology cannot eliminate this access.



2. Cloud-Strategies and Demand

2.1 Hesitance from potential users & on-premises server

The bitkom association hosted a survey in 2024 lead by the question: Which cloud strategy would best fit your corporation?



What companies are looking for: A package that seamlessly integrates the benefits of cloud computing with on-premises solutions.

2.2 Verifiable Digital Sovereignty

Definition „Digital Sovereignty“

via the German Federal Ministry for Digitalization: Users should be able to perform their digital duties

- Independently
- Self-determined
- Securely

For practical purposes, these definitions are too loose.

Definition „Verifiable digital sovereignty“ reinforces:

1. Protection against manipulation, enforcing trust and integrity
(Confidential Computing)
2. Strong protection against data-loss
(Backups independent from the primary provider and cryptographic resilience)
3. Strong and constant access to the service and testable service-switching-opportunities
(Usage with benefits in Open Source Software)

3. Solutions and EU-Innovation

In the cloud sector, experts doubt that innovations outside of the major players (Amazon Web Services (US), Microsoft Azure (US), Google Cloud (US), and Alibaba (CN)) could be successful. The technological advantage resulting from the financial power of these companies is simply too overwhelming. One must, experts say, come to terms with the ever-present possibility of industrial espionage and surveillance.

Other data protection stakeholders are attempting to enforce European data protection standards through legal means. In particular, the European Court of Justice's Schremms I and Schremms II rulings require the regulations governing transatlantic data exchange to be redefined.

By boldly developing innovative cloud technology and establishing a novel operating concept, competitive cloud platforms can be created. Such innovations can satisfy the demand for sustainable computing and address the need for infrastructure to securely process particularly sensitive data.

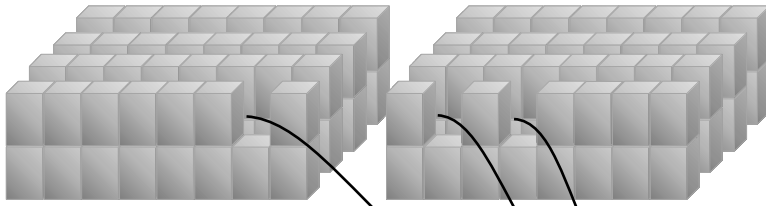
- 3.1 We think that for our duties of innovation, sector boundaries must be crossed to create room for competition.**
- 3.2 To utilize the strength of the entire industry, we integrate open source software with our solutions.**
- 3.3 We try to anticipate the generation after the next's technology, which allows us to always remain technologically ahead.**

»» *Cloud-Servers should be utilized in locations where the heat they generate can be efficiently used, and where regeneratively generated electricity (as much as possible not via the power grid), is available.*

Dr. Hubert Jäger, co-founder and managing director of the real-cis GmbH



4. Distributing Servers



Data centres with thousands of servers will no longer be the only infrastructure for cloud services.

Both through technology and business innovations, more computational capacity is now found at the edge of networks. We create a “network of clusters” from hundreds of secure and sustainable Edge Cloud Modules.

Tech & Biz



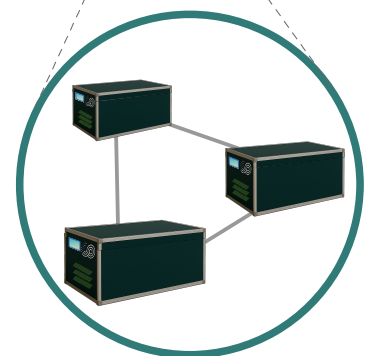
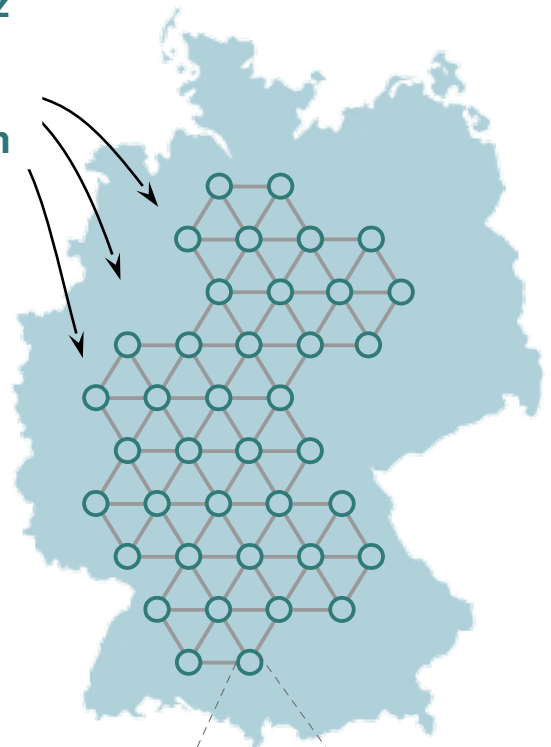
Innovation

4.1 Physical Access Protection Ensures Trust

Since servers outside of data centres are no longer protected by physical access controls, these Edge Cloud Modules require a new type of physical access protection with a so-called cryptographic perimeter seal. This protection thwarts even the most sophisticated attempts to attack the integrity of the servers.

4.2 Two types of novel Edge Cloud Modules

The modules are designed in a way that a simple plug-and-play installation is possible. Its air cooling allows computation power to be placed anywhere where regenerative electricity is available.

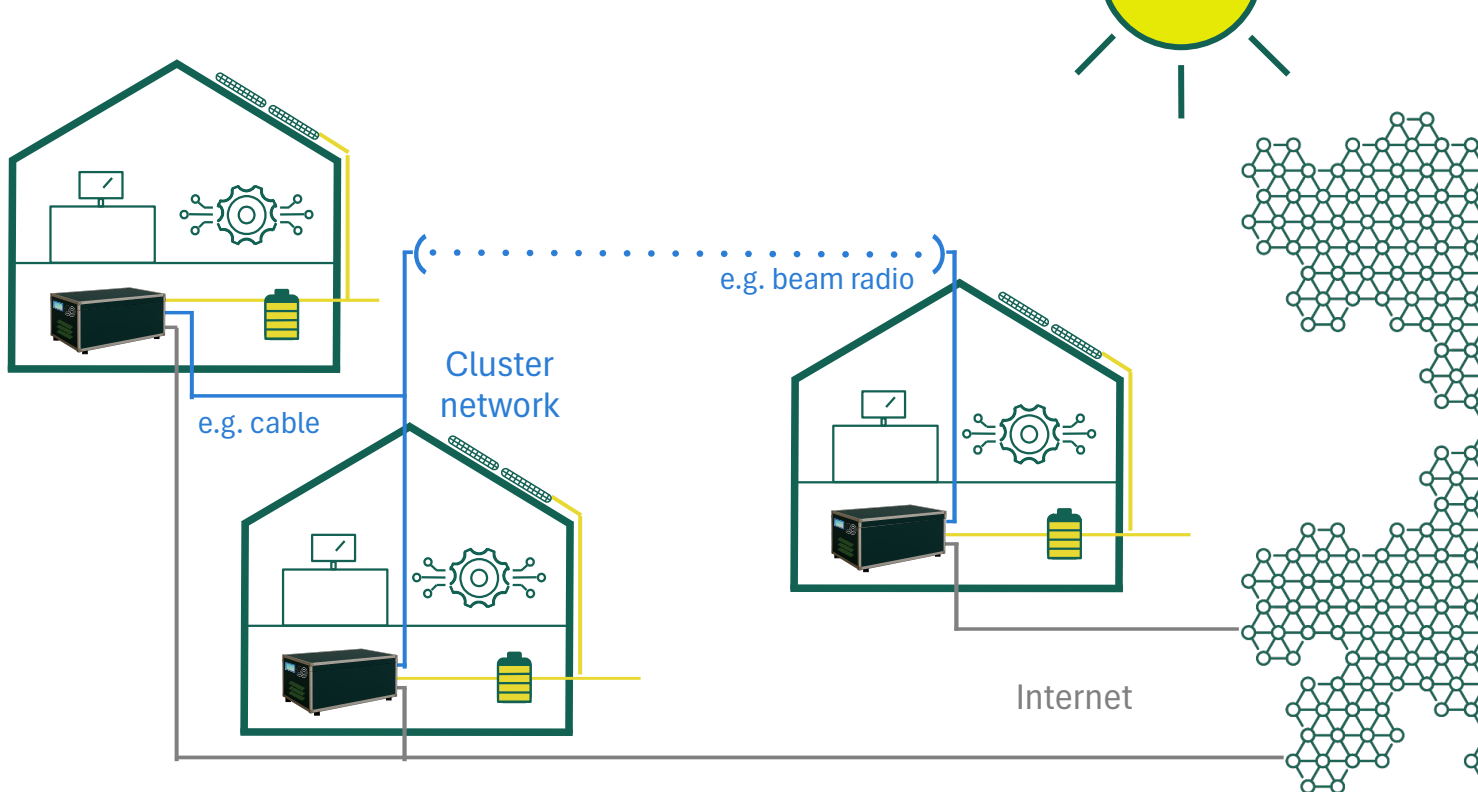


Clusters of multiple Edge Cloud Modules

4.3 Symbiosis with Photovoltaics

The best solution to make computing sustainable is to operate the cloud servers directly where renewable electricity is locally available, so that the power grid is neither burdened nor has to be paid for. Furthermore, royalties could be received for electricity consumed by external workloads. Additionally, the profitable service life of the servers is extended, as there is no pressure to replace them early as in data centers.

On-premises use with own hardware is also possible for machines and IoT devices that are isolated from the internet.



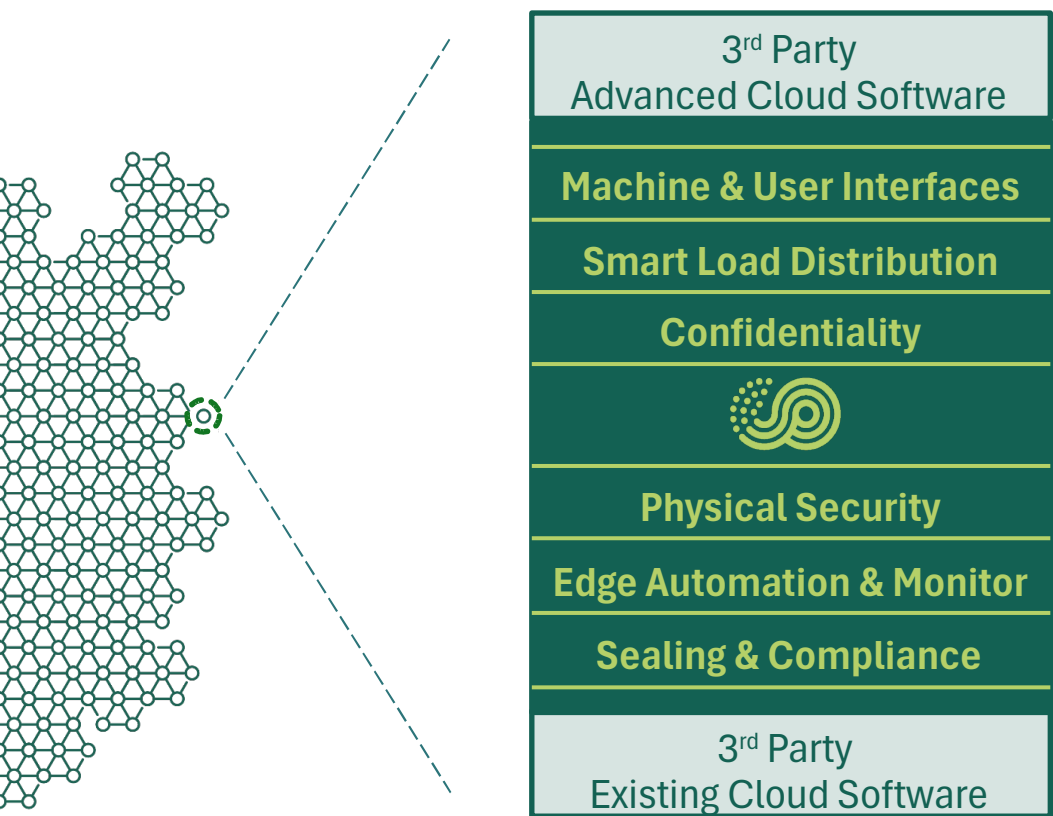
4.4 Best Practice Confidential Computing

The greatest threats to the confidentiality and integrity of data and execution logic do not come from physical manipulation of the infrastructure, but from cyberattacks that are possible through vulnerabilities in the operating system and/or application software. Such security vulnerabilities have either been discovered recently and are so new that they are currently known only to the attackers ("zero-day exploits"). Otherwise, the vulnerabilities have been known for some time but have not yet been addressed through software fixes.

The best protection against the threats posed by these vulnerabilities is so-called confidential computing, which encrypts data not only during transmission to the servers and during permanent storage, but also during processing in memory and on the system buses. This prevents attackers from gaining logical control over the servers, but also from accessing the software processing the data and user data.

4.5 Perfect Root of Trust

Best practice in confidential computing requires that all data and software outside of the processing unit is encrypted and tamper-proof. It also means that the keys protecting the data stored in permanent memory are inaccessible to anyone. To meet these standards for highly available cloud services, a shared, highly trusted source of keys known as the "root of trust" is required. Since no one can gain knowledge of cryptographic secrets even during initialization, and the source can scale up for maximum resilience, it is referred to as a "perfect root of trust."



4.6 Verifying Integrity Cryptographically

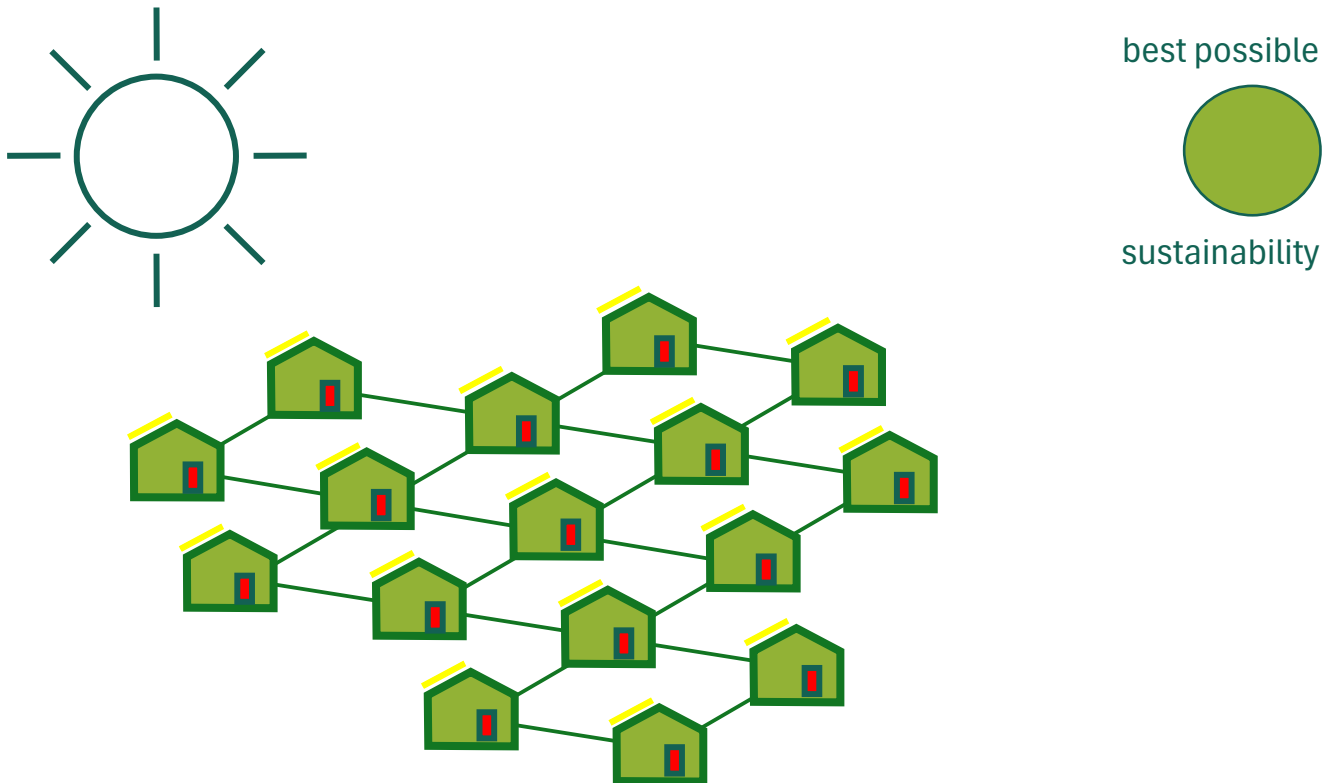
Until now, a user of a cloud service could only verify the trustworthiness and integrity of the service by relying on the cloud provider's statements and the corresponding internet address. The so-called "attestation" in confidential computing offers users the opportunity to verify, with cryptographic rigerosity, that the software has not been tampered with, and is running on secure processors.

4.7 Automation Reduces Labor Cost

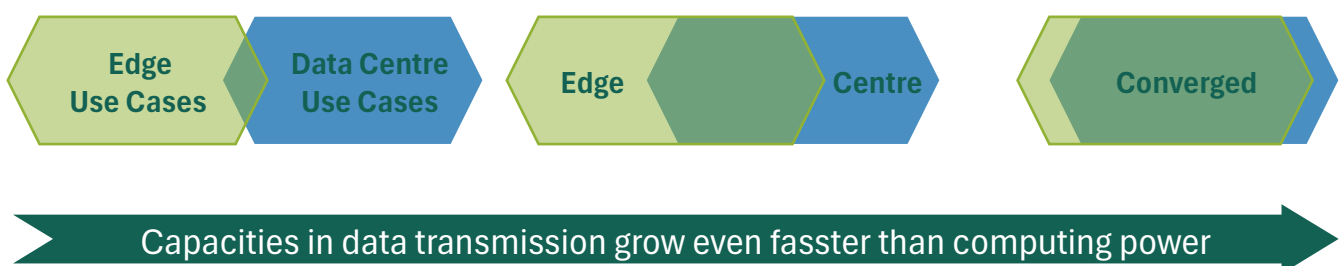
Because the server modules are manufactured centrally and serviced after a lifecycle, no on-site IT personnel are required for commissioning or replacement. The modules integrate automatically into a network of modules. Additionally a cryptographic seal on each module guarantees security against tampering.

5. This is how the Future of the Cloud Looks

5.1 Less data centres, more distribution



5.2 Everything Depends on the Connection



Distributing cloud servers across geographically dispersed locations offers the aforementioned energy and economic advantages, but also poses challenges for networking the server infrastructure. In the medium and long term, a more advantageous ratio of digital transmission capacity to computing capacity can be expected. This is due to the so-called "Moore's Law," which "dictates" that computing power per cost doubles every two years. Digital transmission capacity per cost even triples over the same period.

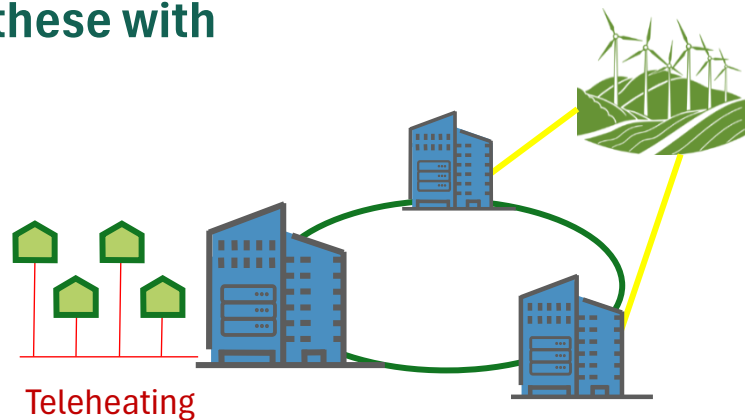
In Edge Clouds, multiple modules are networked together as a cluster within a campus. Within these clusters, the modules are set up in rooms with as independent power supplies as possible, in different fire zones and independent internet access.

Less Data centres, but these with better sustainability.

sustainability



can only be partially increased



Like conventional cloud services, edge cloud services can be offered in an identical manner, provided that the network capacity is not exceeded.






5.3 Rise Resilience of Critical Infrastructure

Another advantage of distributing and networking computing resources is that it avoids risks associated with the concentration of critical infrastructure in one or two data centers. Distributing resources strengthens resilience.

5.4 Your Benefits are to Start Today



BetterEdge
Verifiable Sovereign Computing

-  Structurally more cost-effective than a data-centre-cloud
-  Offers verifiable sovereignty of data and computational resources
-  Eliminates security concerns (Confidential Computing)
-  Arrives with „cloud native“-interface portability
-  As sustainable as can be

5.4 Your Benefits are to Start Today (continued)

Case 1:

You currently operate software on-premises for security reasons:

- You simplify your installation processes and further increase security
- You improve the utilization of your hardware and thus save server cost
- You can scale your workload comparable to a data centre cloud and receive royalties for the capacities of your servers that you make available to third parties

Case 2:

You don't want to install your own hardware but are looking for computing capacity that can be claimed as a Green Asset:

- CO₂ emissions related to IT and cloud are immediately reduced
- You register your progressive actions with your bank as a "Green Asset"
- You present sustainability (climate friendliness and security) as a performance feature for your customers

Case 3:

You don't want to install your own hardware but are looking for computing capacity that meets the highest security requirements and can be operated with full sovereignty:

- Best practice confidential computing technically excludes the operator
- You can set up an independent data backup with cryptographic resilience
- You can cryptographically prove confidentiality and software integrity to your customers



**Operator Cannot
View Data**



**EU law
fully enforceable**



**Shielded from
Manipulation**



**Heat from the
Cloud**



**Symbiosis with
Solar Energy**



**Saving CO₂
through longevity**

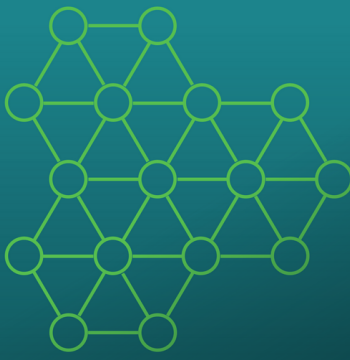




BetterEdge

Verifiable Sovereign Computing

Cloud As It Should Be

Lowest Carbon Design & Security-First Architecture



**BetterEdge**
Verifiable Sovereign Computing

EN


Sign in to continue

TOTP

[Forgot Password?](#)

[Sign In](#)

[Learn More](#)

© 2025  real-cis

Trusted Execution Domains (TEDaaS)



With "Confidential Computing" protected "Virtual Machines" as secure execution environments for IT-use cases or software for SaaS-applications.

Services planned to be available in the future:



Database
as a Service



Backup
as a Service



Functions
as a Service



Acceleration
as a Service

FAQ:

What concrete options for evaluating the offer already exist?

- Prototype operation of a workload (a software, an application, possibly from a partner) for an agreed period with coordinated Service Level Agreements
- Prototype operation of the confidential computing system software in your data centre. Operation of any number of secured execution environments
- Prototype operation of an air-cooled edge cloud module, prototype operation of workload on this module
- Prototype operation of a heat-coupling module, prototype integration into the heating infrastructure, and prototype operation of workload on this module
- Planning of real estate developments

Which business models are generally available for partners?

- Booking of cloud computing power with real-cis
- Purchase of edge cloud modules operated by real-cis on your behalf, with lucrative royalties on cloud services provided to third parties using your hardware (€1/kWh)
- Operation of your own edge cloud for "Verifiable Sovereign Computing"

Definitions:

“Cloud” — Provision of computing power over the internet as a service

“Data Centre Cloud” — Provision of computing power as a service from data centres

“Edge Computing” — Use of computing power outside data centres or in devices

“Edge Cloud” — Provision of computing power as a service from outside data centres

“Cloud Edge Continuum” — Cloud with resources both inside and outside data centres

“IaaS” — Infrastructure as a Service

“PaaS” — Platform as a Service

“XaaS” — X-things as a Service (Database as a Service, Functions as a Service, etc.)

“SaaS” — Software (IT applications) as a Service

“cloud native” — Extensive abstraction of infrastructure through cloud services for operating scalable applications

“Hyperscaler” — Extremely large-scale Cloud Service Providers (CSP)



BetterEdge
Verifiable Sovereign Computing

real-cis GmbH
Munich • Frankfurt
Rheinstr. 5, Langen 63225 GERMANY
info@real-cis.com, www.real-cis.com
+49 6103 90298-0