UNiSCON
Sealed Cloud Technologies

A member of TÜV SÜD

SEALED PLATFORM

The ultra secure cloud platform for the enterprise

uniscon.com

SEALED PLATFORM – THE ULTRA SECURE CLOUD PLATFORM

Protect your data & applications in the cloud!

Sealed Platform is the Ultra Secure Cloud Platform for your data and applications. Sealed Platform's unique Zero Priviledged Access Architecture securely guards against unauthorized access of your data and applications in the cloud

Easily and securely move your legacy applications to the cloud!

Sealed Platform can run virtually any application without code modification and instantly provides security and compliance with data privacy laws (GDPR)

SEALED PLATFORM

No privileged access for providers or administrators

Nobody except the data owner has access

Protection of application-data and meta-data

Sealed Platform enables highly secure processing of non-encrypted data in the cloud

Encryption of data at rest without a master key

Impossible to decrypt the data without the user credentials

Sealed Platform – the ultimate security upgrade for your business applications

Sealed Platform is a top-security cloud platform suitable for running diverse applications with high demands on data security. It is capable of operating as a private, hybrid or public cloud platform for:

- **Enterprises**
- **Platform Provider / Telco Provider**
- **Independent Software Vendor (ISV)**

SEALED PLATFORM – THE ULTRA SECURE CLOUD PLATFORM

How does Sealed Platform protect your data and applications?

Data Clean-Up Areas

When a breach is detected:

- Sessions are transferred to other segments
- The power of disk-less servers is shut-down
- All unencrypted data is deleted

Key Distribution Options

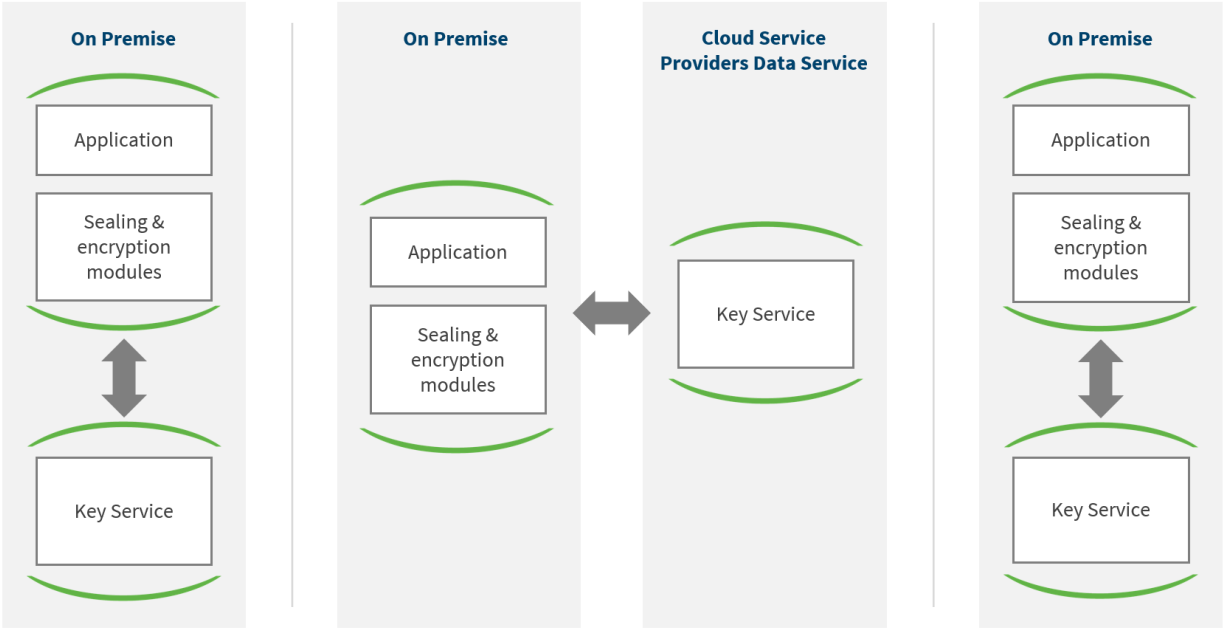
- Keys are generated from user secrets
- Keys are auto-generated and never leave the Data Clean-up Area

Integrity Assurance

Independent Contributors/Auditors participate/surveil/confirm:

- No SSH access
- Filtered Operational & Maintenance Access (OMA)
- Multi Party Rack and Server Sealing
- Signing of Software/Trusted Boot
- Integrity of Setup

Deployment options in a private, hybrid or public cloud



Private Hybrid Public

Minimum requirements for Sealed Platform

Programming Language	Any
File System	Any
Message Brokers	Any
Data Base	Must support Transparent Data Encryption (TDE)
OS	Linux
Operational mode	Docker, Trustme* or OpenStack
Application Security	No sensitive data in logfiles
Rights and roles concept	Strict application of need-to-know principle

*Trustme is an ultra-secure container technology of Fraunhofer AISEC, used by Uniscon in the frame of the services for the International Data Space Association

PRIVACY BY DESIGN AND OPERATIONAL EXCELLENCE

Your benefits with zero-knowledge Sealed Platform

Reputation
- Communicate top security
- Communicate technology lead
- Dramatically reduce risk for publically known breaches

Savings
- Expensive organisational measures are replaced by technical
- Lean control of processor
- Reduced inspection effort in IT-audits

Compliance
- Data protection (GDPR)
- Data minimization for admins acc. to the State-of-the-Art
- Trade secrecy (upcoming GeschGehG) & Professional secrecy (§ 203 StGB)

Start your free proof of concept

1. Go to **uniscon.de/en/sealed-platform-poc/**
2. Please clarify software requirements
3. Give us some input how you want to run Sealed-Platform
4. After submitting your information
   - we send you some information about the PoC-On-boarding process and
   - a Sealed Platform Consultant from Uniscon will contact you.

Contact
Uniscon GmbH
Agnes-Pockels-Bogen 1
80992 Munich | Germany

Web www.uniscon.com
Email contact@uniscon.de
Phone +49 (0)89 4161 5988 100