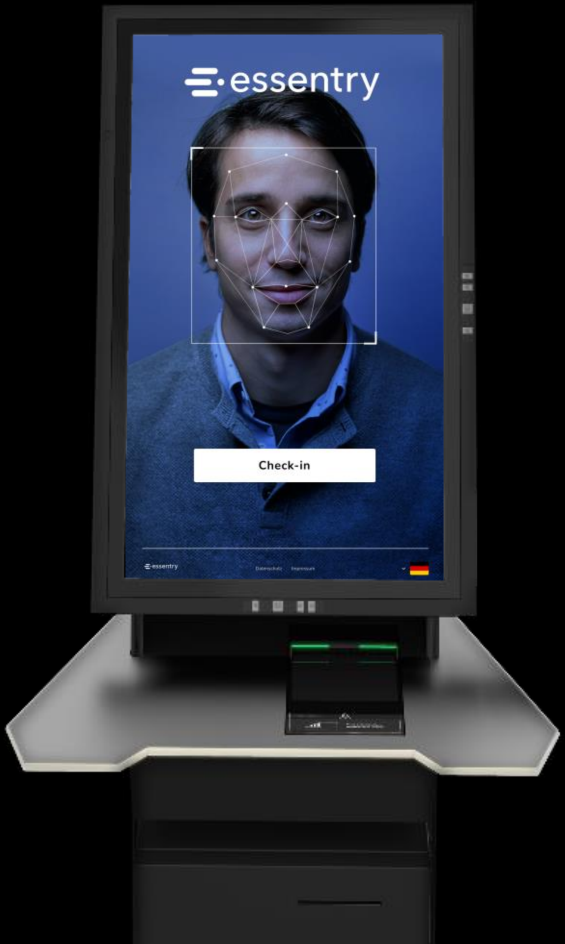
essentry

Berlin, 01.02.2024

essentry
Data Protection Concept



The data protection concept.

A solution with the highest data protection and data security standards.
Made in Germany.

GDPR compliant.

essentry meets the strict requirements of the EU's General Data Protection Regulation and is continuously audited by an independent external data protection officer.

Full data control.

essentry gives you full control over your data. You can centrally access the data you need to fulfill audit requirements. At the same time, predefined deletion mechanisms ensure compliance with legal requirements.

Encryption.

essentry uses strong encryption algorithms to protect data both "in transit" and "at rest“. All databases are encrypted with AES-256, HTTPS is used for browser connections, and developers use SSH, SSL / TLS to connect to essentry systems.

Certified infrastructure.

essentry uses industry-leading cloud infrastructure that meets the highest security and availability standards. Our third-party certifications include ISO 27001, ISO 27017, ISO 27018, SOC2.

Highly secure, enterprise-grade infrastructure.

Enterprise-grade infrastructure.

Essentry GmbH is ISO 27001 certified on the basis of BSI IT-Grundschutz (BSI-IGZ-0459-2021).
essentry servers are hosted in SOC 2 Type II and ISO 27001 certified facilities in the Frankfurt (Germany) region.

Our data center facilities are secured with a perimeter of multi-level security zones, 24/7 manned security forces and CCTV video surveillance. They are secured by multi-factor identification with biometric access control, physical locks and alarm systems in case of security breaches.

Data encryption.

The communication between the user and the essentry servers is encrypted according to industry best practices: HTTPS and Transport Layer Security (TLS) over public networks. Qualys' SSL labs have rated our servers Level A+. In addition, when using our Windows kiosk, the total network traffic is routed via our IPSec VPN. The hard drives of all servers are encrypted according to AES-256.

High availability.

essentry offers a highly available service. Should an incident occur, we have comprehensive incident response and customer notification procedures in place. We have a 24/7 service center and offer an onsite service for hardware-related issues with a 24x7x4 hour availability.

Third-party penetration testing.

In addition to our extensive internal scanning and testing program, penetration tests are performed by selected service providers. essentry contracts third-party security experts to conduct a thorough annual penetration test for the entire essentry service offering.

Privacy-by-Design.

Compliance standards

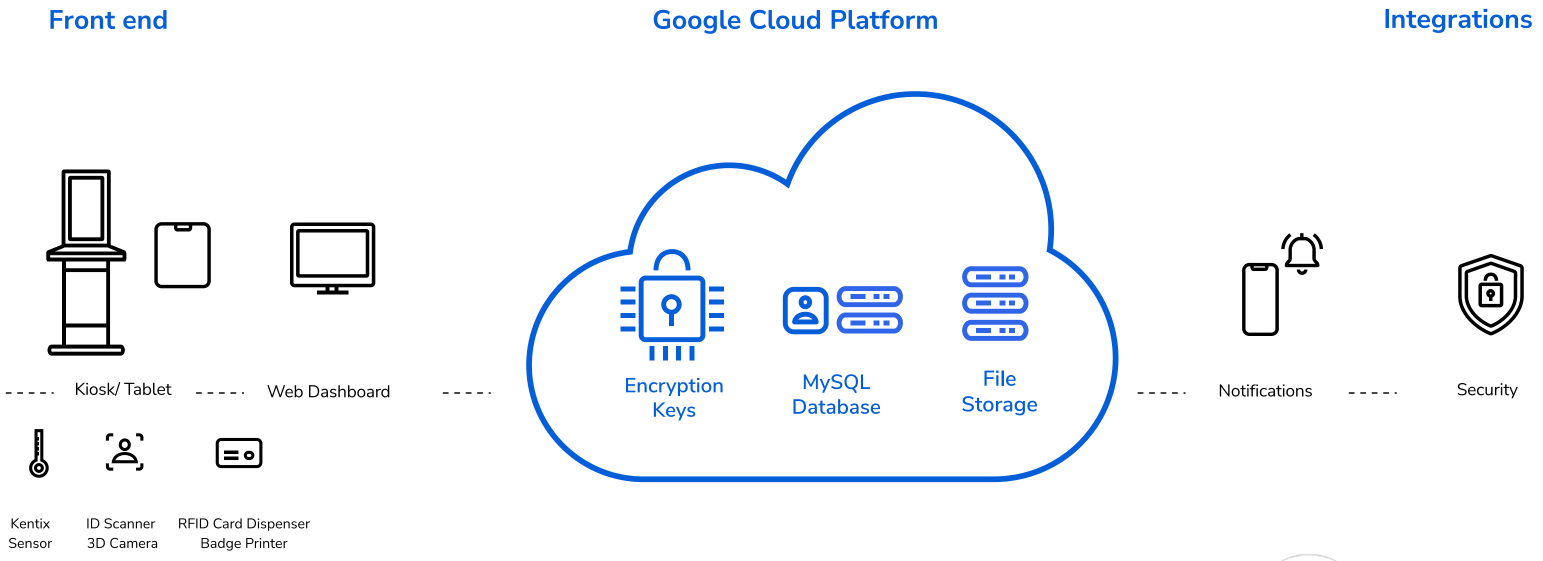
At essentry, data privacy is a priority. We value our customers' trust and will ensure their visitor data is protected. We demonstrate our commitment to privacy preservation in both our processes and technical application design. We pursue a systematic privacy-by-design strategy.

Established and often manual processes	What essentry does	What essentry does not do
Insufficient verification of the identity document (ID)	✓ Verification of the identity document (ID) locally	✗ Verification of the identity document (ID) in the cloud
Manual face match	✓ 1:1 face match	✗ 1:n facial recognition
Manual data processing and non-transparent retention policies	✓ Advanced privacy rights and transparent retention policies	✗ Same privacy rights for everyone and infinite data retention
Non-transparent privacy policy and user consent	✓ Clear privacy policy and user consent	✗ Processing sensitive data without given consent

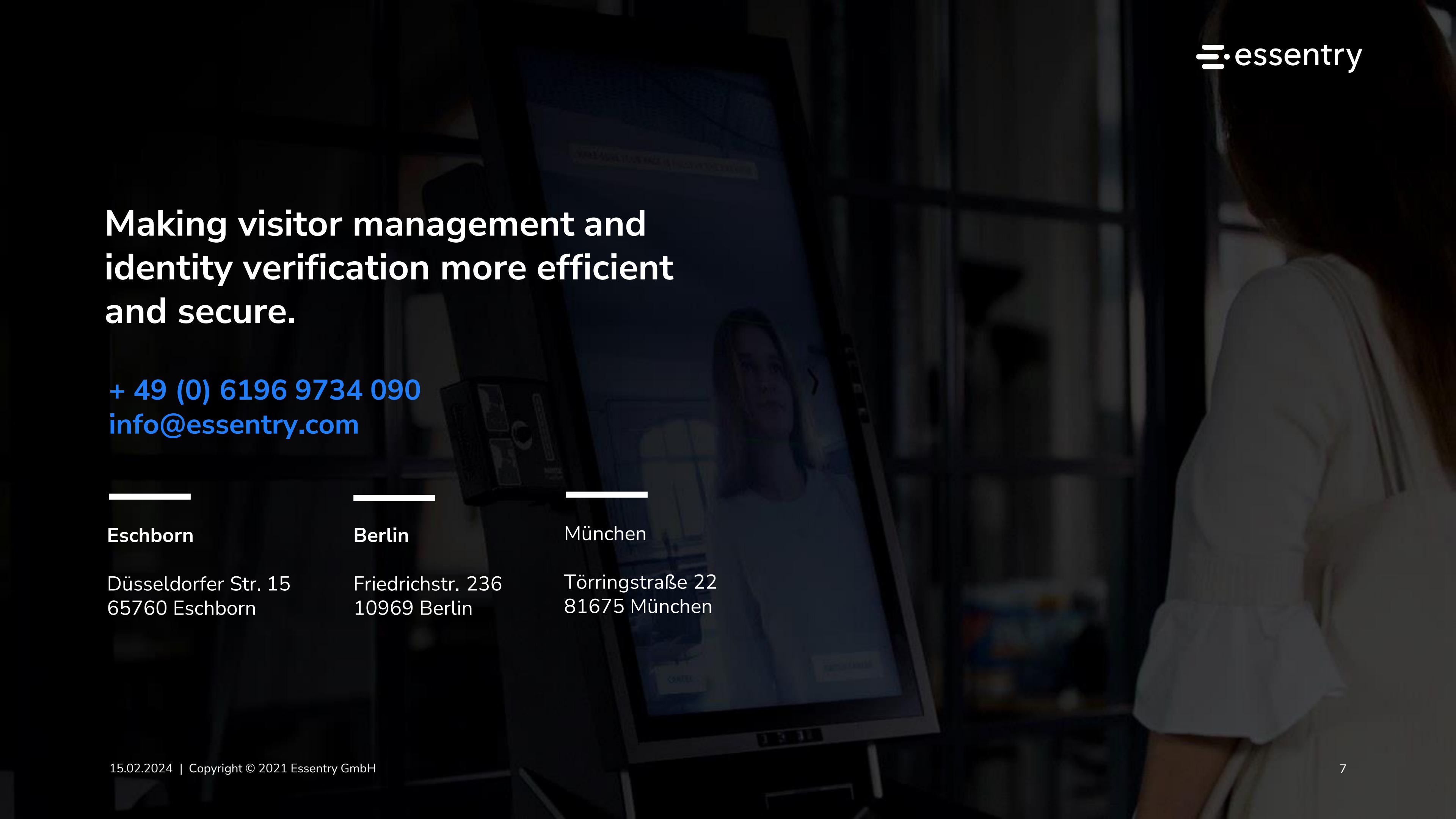
Privacy-by-Design.

Established and often manual processes	What essentry does	What essentry does not do
Insufficient verification of the identity document (ID) Typically, humans are not able to verify IDs from all different countries and check whether the ID contains all the important security features. Additionally, it is not a welcoming user experience to have to hand over one's own identity card to another person for verification purposes.	✓ **Onsite verification of the identification document (ID)** In order to reliably verify an ID, the essentry kiosk checks for individual security features using three different light sources. The data is only processed with the user's consent and is deleted immediately after verification.	✗ **Verification of the identity document (ID) in the cloud** essentry never stores images of the full ID in its records – neither locally nor in the cloud. The verification of the ID only takes place locally. If required, only the person's picture on the ID is matched with the picture of the person in front of the kiosk.
Manual face match The human eye performing face matches has proven to be significantly more error-prone than face matches conducted by computer-based algorithms.	✓ **1:1 face matching** essentry compares the image of the ID document with a 3D photo of the person in front of the kiosk taken on site. We rely on proven algorithms to ensure the utmost accuracy when performing this comparison.	✗ **1:n facial recognition** essentry never matches a photo against a larger database to verify photos and identities.
Manual data processing and non-transparent retention policies Typically, visitor data is stored and shared in multiple systems or paper logbooks, to which multiple people have access. Retention and deletion policies of these systems are often neither transparent nor are they enforced.	✓ **Comprehensive data protection rights and transparent storage guidelines** essentry is subject to strict requirements concerning data protection. The way the technology is designed plays a special role in ensuring the security of the data. The customer decides which data is stored and when it is deleted. The essentry platform provides a transparent overview of retention periods and deletion rules at all times.	✗ **Same privacy rights for everyone and infinite data retention** With essentry, limited access to necessary information is based on permissions and what designated individuals are allowed to see. essentry strictly follows GDPR data protection regulations including transparent retention policies.
Non-transparent privacy policy and user consent If displayed at all, privacy policies are typically only shown on paper (small font and/or back of page) and user consent is not centrally stored and, as a result, is not retraceable (e.g., for audits).	✓ **Clear privacy policy and user consent process** Data protection is a top priority at essentry. We inform the user about the individual privacy policy at various points of contact. For example, the invitation email contains a link to the privacy policy. When checking in at the kiosk, the guest directly consents to data processing before the identity check takes place.	✗ **Processing sensitive data without given consent** essentry does not process sensitive data at any time prior to consent. Only after the user has accepted the privacy policy and given their consent, will we initiate the verification process.

Platform-Architektur.



essentry is BSI-certified



Making visitor management and identity verification more efficient and secure.

+ 49 (0) 6196 9734 090
info@essentry.com

Eschborn

Düsseldorfer Str. 15
65760 Eschborn

Berlin

Friedrichstr. 236
10969 Berlin

München

Törringstraße 22
81675 München

essentry

Disclaimer

The material in this presentation has been prepared by Essentry GmbH and is general background information about essentry's activities current as at the date of this presentation. This information is given in summary form and does not purport to be complete. The content of this presentation is proprietary and confidential information of Essentry GmbH. It is not indented to be distributed to any third party without the written consent.