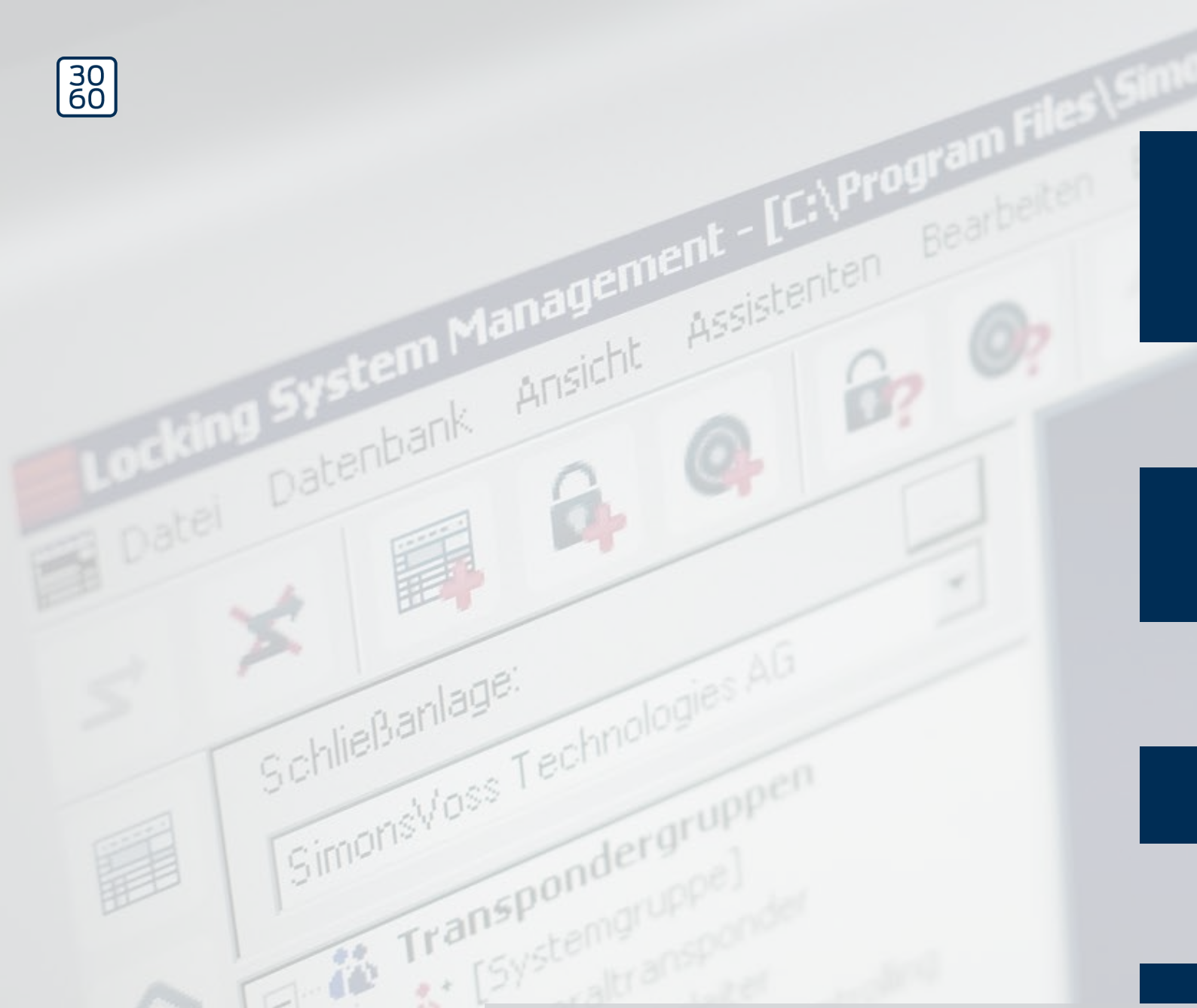

Protezione dei dati nei sistemi SimonsVoss

Informazione

21.01.2025

SimonsVoss technologies

Sommario

1. Protezione base IT 3
1.1 Quali sono i requisiti di protezione dei dati elaborati nel sistema? 3
1.2 Quali sono i requisiti raccomandati per l'infrastruttura IT? 3
2. Codifica 4
2.1 I dati del Sistema 3060 sono criptati? 4
2.2 Quali dati vengono criptati durante il processo? 4
2.3 Anche i percorsi di trasmissione, ad esempio via radio, sono criptati? 4
3. Metodi di lavoro conformi alla protezione dei dati secondo il RGPD 5
3.1 Quali dati personali vengono memorizzati nel software? 5
3.2 Per quale finalità i dati personali vengono memorizzati nel software? 5
3.3 Per quanto tempo i dati personali sono memorizzati nel software? 5
3.4 Il diritto di leggere le liste di accesso può essere ulteriormente garantito? 6
3.5 I dati personali memorizzati nel software sono protetti dall'accesso di terzi? 6
3.6 Può essere messa a disposizione una copia dei dati memorizzati? 6
3.7 I dati personali possono essere cancellati dal software? 6
4. Supporto e ulteriori informazioni 7

1. Protezione base IT

1.1 Quali sono i requisiti di protezione dei dati elaborati nel sistema?

In generale, nel software vengono elaborati e memorizzati solo dati non critici con requisiti di protezione cosiddetti normali. In altre parole, dati la cui ipotetica perdita non danneggerebbe la reputazione di una persona o l'immagine di un'azienda. E nemmeno un danno finanziario elevato.

1.2 Quali sono i requisiti raccomandati per l'infrastruttura IT?

Secondo l'Ufficio federale per la sicurezza informatica (BSI), una protezione informatica di base come concetto di sicurezza è sufficiente per un sistema di chiusura SimonsVoss ed è considerata il requisito minimo raccomandato per la vostra infrastruttura informatica.

2. Codifica

2.1 I dati del Sistema 3060 sono criptati?

Sì. All'interno della comunicazione del sistema, i pacchetti di dati sono criptati end-to-end. Si impiegano metodi di protezione dei dati a più livelli, garantiti in ultima istanza con una procedura di crittografia standard (AES, 3DES). Le versioni più recenti dei nostri prodotti innalzano il livello di sicurezza, in quanto sono sottoposte a un aggiornamento tecnico continuo.

NOTA

Password dell'impianto di chiusura integrata nel concetto di sicurezza

La password dell'impianto di chiusura assegnata dal cliente (non utente) è integrata nell'intero concetto di sicurezza. Con una password complessa si incrementa automaticamente anche la lunghezza di chiave della procedura di crittografia impiegata e quindi la sicurezza dei dati. A tale riguardo si consigliano password di almeno 12 caratteri, contenenti numeri, lettere minuscole, maiuscole e segni speciali. Conservare la password dell'impianto di chiusura in un luogo sicuro (ad es. la cassaforte), a cui possano accedere unicamente le persone autorizzate.

2.2 Quali dati vengono criptati durante il processo?

Nessun dato personale viene trattato nell'ambito della comunicazione del sistema, ma viene pseudonimizzato con l'aiuto di numeri di identificazione. Anche senza crittografia, non è possibile attribuire il nome a una persona reale.

2.3 Anche i percorsi di trasmissione, ad esempio via radio, sono criptati?

No. Grazie all'impiego sistematico della crittografia end-to-end la comunicazione può avvenire in sicurezza indipendentemente dal percorso di trasmissione. I dati intercettati non possono essere letti senza l'apposita chiave segreta. Con la crittografia end-to-end è possibile utilizzare percorsi di trasmissione propri del sistema senza perdite di potenza.

3. Metodi di lavoro conformi alla protezione dei dati secondo il RGPD

3.1 Quali dati personali vengono memorizzati nel software?

Vi è la possibilità di memorizzare i seguenti dati personali nel software:

- Nome
- Cognome*
- Qualifica
- Indirizzo
- Telefono
- Indirizzo email
- Numero personale*
- Nome utente
- Reparto
- Luogo/edificio
- Impostato da/a
- Data di nascita
- Centro di costo
- Foto

Di questi dati solo il cognome e il numero personale sono *campi obbligatori e sono necessari per l'utilizzo del software.

Ai sensi dell'art. 9 del RGPD non vengono memorizzate categorie particolarmente sensibili di dati personali.

3.2 Per quale finalità i dati personali vengono memorizzati nel software?

Per poter utilizzare nella loro completezza le funzioni di un impianto di chiusura elettronico è necessario poter assegnare a un determinato utente (ad es. un collaboratore) i supporti di identificazione utilizzati (ad es. transponder).

3.3 Per quanto tempo i dati personali sono memorizzati nel software?

I dati vengono memorizzati almeno per la durata di utilizzo di un supporto di identificazione all'interno dell'impianto di chiusura (ad es. appartenenza a una società).

La durata di conservazione dei dati (ad es. nelle registrazioni e gli elenchi di accesso) può essere modificata dal gestore dell'impianto di chiusura e adattata alle indicazioni aziendali.

3.4 Il diritto di leggere le liste di accesso può essere ulteriormente garantito?

Quando si utilizza la funzione opzionale ZK nei nostri componenti di chiusura, l'accesso ai dati raccolti con essa può essere dotato di maggiori diritti di utilizzo.

Esempio: viene creato un utente separato per il consiglio di fabbrica. Solo a questo utente vengono concessi i diritti di lettura degli elenchi di accesso in caso di sospetto. Inoltre, questo utente può essere protetto con una password condivisa. Solo una parte della password è nota a due o più membri del consiglio di fabbrica.

3.5 I dati personali memorizzati nel software sono protetti dall'accesso di terzi?

Fondamentalmente l'utente (il cliente finale) dell'impianto di chiusura e del software è responsabile della gestione e della messa in sicurezza dei diritti di accesso.

Nel sistema di chiusura stesso tutti i dati sono protetti da metodi crittografici articolati in vari livelli. Non è possibile aprire l'interfaccia grafica utente, per poter accedere ai dati, senza una password e i relativi diritti utente.

Nell'ambito della gestione delle attività non avvengono la trasmissione automatica a terzi, l'utilizzo o l'elaborazione da parte di SimonsVoss.

3.6 Può essere messa a disposizione una copia dei dati memorizzati?

Tutti i dati raccolti relativi a una persona interessata (a partire dalla versione 3.4), presupposti i relativi diritti di utilizzo, possono essere messi a disposizione come copia da parte del cliente (ad es. nell'ambito di un audit) tramite la funzione Esporta. Ciò permette al cliente di osservare il diritto di accesso ai sensi dell'art. 15, comma 3 del RGPD.

3.7 I dati personali possono essere cancellati dal software?

I dati personali possono essere cancellati definitivamente dal software (a partire dalla versione 3.4 SP) e dalla relativa banca dati da parte del cliente su richiesta di una persona interessata ai sensi dell'art. 17 del RGPD.

4. Supporto e ulteriori informazioni

Materiale informativo/Documenti

Maggiori informazioni sul funzionamento e sulla configurazione nonché ulteriori documenti sono riportati nella homepage:

https://www.simons-voss.com/it/documenti.html

Software e driver

Software e driver sono disponibili sulla homepage:

https://www.simons-voss.com/it/assistenza/download-software.html

Dichiarazioni di conformità

Le dichiarazioni di conformità e altri certificati sono riportate nella homepage:

https://www.simons-voss.com/it/certificati.html

Supporto tecnico

Il nostro supporto tecnico sarà lieto di aiutarvi (linea fissa, i costi dipendono dal provider):

+49 (0) 89 / 99 228 333

E-mail

Se si preferisce contattarci via e-mail, scrivere all'indirizzo:

support-simonsvoss@allegion.com

FAQ

Per informazioni e consigli utili, consultare l'area FAQ:

https://faq.simons-voss.com/otrs/public.pl

Indirizzo

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Germania

SimonsVoss Technologies GmbH, Feringastr. 4, D-85774 Unterfoehring, Germania

Ecco a voi SimonsVoss

SimonsVoss, pioniere della tecnologia di chiusura radiocomandata senza fili, offre soluzioni di sistema con un'ampia gamma di prodotti per il settore SOHO, per le piccole e grandi imprese e le istituzioni pubbliche. Gli apparati SimonsVoss racchiudono funzionalità intelligenti, alta qualità e design pluripremiato Made in Germany.

Come fornitore di prodotti innovativi, SimonsVoss punta su scalabilità, alta sicurezza, affidabilità, software potenti e facilità d'uso. Questo rende SimonsVoss un leader tecnologico riconosciuto nell'ambito dei sistemi di chiusura digitali wireless.

Coraggio di innovare, mentalità e agire sostenibile e grande attenzione verso collaboratori e clienti: questa è la chiave del nostro successo.

SimonsVoss fa parte di ALLEGION, un gruppo internazionale operante nel settore della sicurezza. Allegion vanta sedi in circa 130 paesi (www.allegion.com).

Qualità "made in Germany"

Per SimonsVoss, il "Made in Germany" è un impegno serio: Tutti i prodotti sono sviluppati e realizzati esclusivamente in Germania.

© 2025, SimonsVoss Technologies GmbH, Unterföhring

Tutti i diritti riservati. Testo, immagini ed elaborazioni grafiche sono tutelati dai diritti d'autore.

Il contenuto di presento documento non può essere copiato, divulgato né modificato. Ulteriori informazioni su questo prodotto sono disponibili sul sito web di SimonsVoss. Con riserva di modifiche tecniche.

SimonsVoss e MobileKey sono marchi registrati di SimonsVoss Technologies GmbH.

SimonsVoss technologies

Made in Germany

A BRAND OF ALLEGION