SDoT Secure Integrated Service® & SDoT Secure Depository®

Behandlung von digitalen Verschlusssachen für informationsverarbeitende Systeme

Die VS-Registraturlösung der Firma INFODAS GmbH bildet sowohl die **elektronische** VS-Registratur als auch die **physische** VS-Registratur ab. Damit ist eine durchgängige, medienbruchfreie und transparente VS-Nachweisführung möglich.
Grundlage sind die geltenden Vorschriften der VS-Anweisung (VSA) und die dazugehörigen Durchführungsbestimmungen der A-1130/1 und A-1130/2 – Militärische Sicherheit in der Bundeswehr, der A-960/1 – IT-Sicherheit in der Bundeswehr sowie das Handbuch für den Geheimschutz in der Wirtschaft (Geheimschutzhandbuch).
Im Kern der VS-Registraturlösung steht die elektronische VS-Registratur, die über eine Schnittstelle an das elektronische Tagebuch der physischen VS-Registratur angebunden ist. Über diese Schnittstelle wird die physische und elektronische VS-Bearbeitung zusammengeführt. Es entsteht eine VS-Registratur, die über beide „Welten“ hinweg sicherstellt, dass die VS-Prozesse vorschriftenkonform ausgeführt werden.

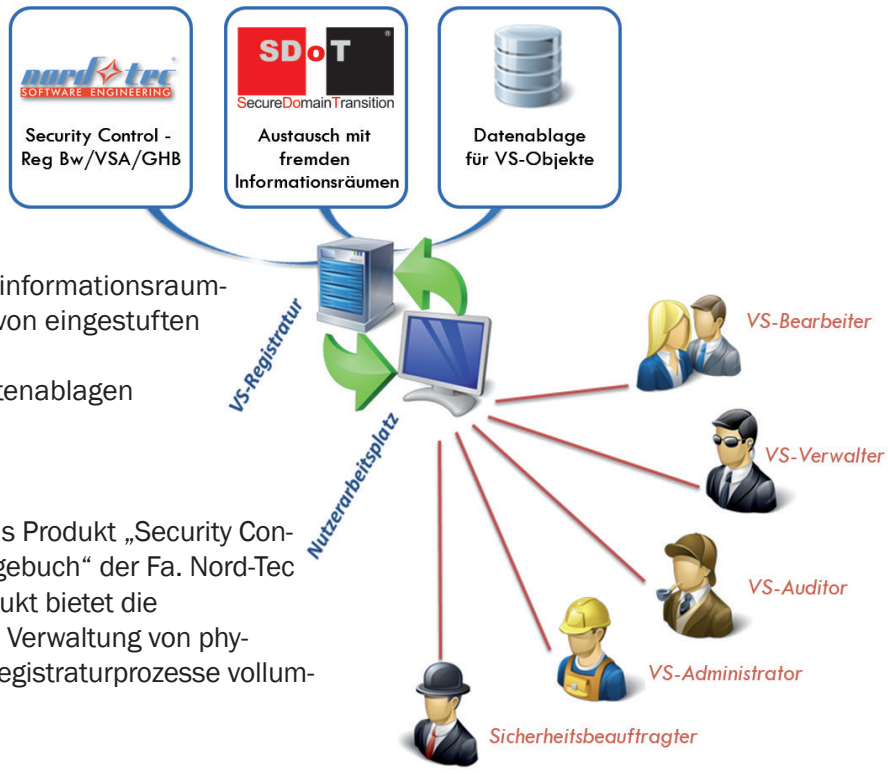
Elektronische VS-Registratur

Die zentrale Serverkomponente bildet den Kern der elektronischen VS-Registratur. Diese besteht aus Teilkomponenten, die folgende Aufgaben erfüllen:

- **SDoT SIS**® bildet die VS-Prozesse ab und führt den VS-Nachweis
- **SDoT SD**® verwaltet flexibel die angeschlossenen Datenablagen

Mit **SDoT SIS**® **& SD**® wird eine elektronische VS-Registratur bereitgestellt, die

- eine Schnittstelle zum elektronischen Tagebuch der physischen VS-Registratur („SeCon-Reg“ der Fa. Nord-Tec) bietet,
- die Anbindung von Security Gateways zum informationsraumübergreifenden elektronischen Austausch von eingestuften Informationsobjekten realisiert und
- die Einbindung von projektspezifischen Datenablagen ermöglicht.



Physische VS-Registratur

Innerhalb der physischen VS-Registratur wird das Produkt „Security Control – Reg Bw/VSA/GHB – Elektronisches VS-Tagebuch“ der Fa. Nord-Tec Software Engineering OHG eingesetzt. Das Produkt bietet die VSA- und ZDv 2/30 konforme Registrierung und Verwaltung von physischer VS und setzt somit alle physischen VS-Registraturprozesse vollumfänglich elektronisch um.

Verteilte Registraturen und Synchronisation

- Verteilte Registraturen werden durch umfassende Replikations- und Synchronisierungsmechanismen unterstützt:
  – Spiegelung der Daten: z.B. Verteilung auf verschiedene RZ-Standorte
  – Bedarfsorientierter Austausch der Daten: z.B. zwischen Heimatland und Einsatzland
- Skalierbarkeit: Über Load Balancing-Mechanismen werden projektspezifische Performance- und Lastanforderungen abgedeckt.

Zugriffskontrolle und Kenntnisnahme

- Bei jedem Zugriff wird die Rolle des Nutzers gegen einen vorhandenen Verzeichnisdienst (online) geprüft.
- Bei jedem Zugriff wird der Nutzer auf Basis des persönlichen Zertifikates authentifiziert.
- Vor jeder Kenntnisnahme wird die Ermächtigung des Nutzers geprüft.
- Vor jeder Kenntnisnahme wird das Need-to-know bzw. Responsibility-to-share des Nutzers geprüft.

Bildung von Referenzen

- Referenzen halten fest, mit welcher VS-Registratur die Verschlusssache ausgetauscht und unter welcher Tagebuch-Nummer (physische VS-Registratur) bzw. elektronischer Dokumenten-ID (elektronische VS-Registratur) die Verschlusssache geführt wird.
- Bei Umstufung einer VS werden mit Hilfe der Referenzen automatisch alle relevanten Registraturen (sowohl elektronisch als auch physisch) benachrichtigt.

Unterstützte Rollen

- Unterstützt werden die folgenden Rollen: VS-Leser, VS-Sachbearbeiter, VS-Verwalter, VS-Auditor, VS-Administrator und Sicherheitsbeauftragter (SiBe).
- Rollen können aus einem vorhandenen Verzeichnisdienst der Einsatzumgebung abgefragt werden.

Allgemeine Sicherheitsmechanismen

- Security Appliance mit gehärtetem und minimalisiertem Linux Betriebssystem (virtualisierter Betrieb möglich).
- Authentifizierung der Nutzer anhand von persönlichen Zertifikaten.
- Nutzung von verschlüsselter Kommunikation (SSL) zur Wahrung von Vertraulichkeit und Integrität.
- Verwendung des SDoT Security Frameworks zur Erfüllung höchster IT-Sicherheitsanforderungen.

Abbildung der Ermächtigungen

- Einem Nutzer übertragene VS-Ermächtigungen werden über so genannte Clearance-Dateien abgebildet. Diese sind durch XML Security Label integritätsgeschützt.
- Clearance-Dateien enthalten den ermächtigten Geheimhaltungsgrad sowie Sperrvermerke.

Verschlüsselung

- In COTS-Produkten (Datenablage/Datentresore) implementierte Verschlüsselungsfunktionen können genutzt werden.
- Unterstützt wird zudem eine austauschbare bzw. projektspezifisch anpassbare transparente Verschlüsselung auf Objekt-Basis (jede Datei wird mittels eines Dokumentenschlüssels einzeln verschlüsselt).

SDoT SIS® & SD® wurde mit der Philosophie entwickelt, sich vollumfänglich in die fachlichen Prozesse und Fachanwendungen zu integrieren.

INFODAS – Gesellschaft für Systementwicklung und Informationsverarbeitung mbH
Rhonestr. 2
50765 Köln
Telefon (0221) 709 12 - 0
Fax (0221) 709 12 - 86
vertrieb@infodas.de
www.infodas.de