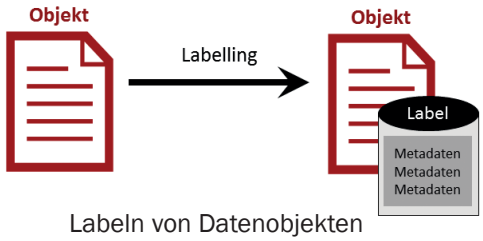
Labelling

Elektronische Kennzeichnung von Datenobjekten als Grundlage für die Filterung an Sicheren Netzübergängen – Einführung

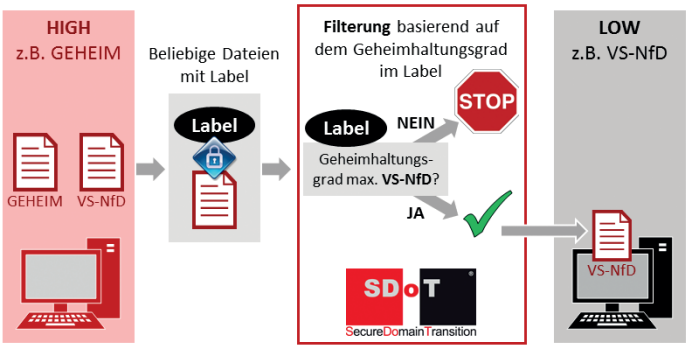
Ein **Security Label** ist eine maschinenlesbare Menge strukturierter Metadaten, die einem Datenobjekt (z. B. einer Datei oder einer elektronischen Nachricht) beigefügt wird, um die Sicherheitsanforderungen an das Datenobjekt zu kennzeichnen.



Labeln von Datenobjekten

In den meisten Anwendungsfällen geht es dabei um die Vertraulichkeit des Datenobjekts. Das Security Label beinhaltet dann den **Geheimhaltungsgrad** (z.B. VS-VERTRAULICH oder GEHEIM) des Datenobjekts und ggf. **Warn- und Zusatzvermerke** bzw. besondere Behandlungskennzeichnungen (z.B. „Nur Deutschen zur Kenntnis“ oder „KRYPTOSICHERHEIT“).

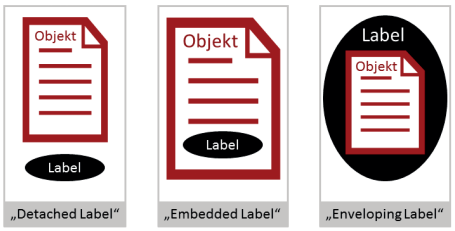
Wenn solchermaßen gekennzeichnete („gelabelte“) Datenobjekte in andere Netze übertragen werden, können **Sicherheitsgateways** die Security Label auswerten und auf dieser Basis automatisch entscheiden, ob das Datenobjekt weitergeleitet werden darf: Ist die VS-Einstufung des Datenobjekts höher als die des Zielnetzwerks, blockiert das Sicherheitsgateway die Datenübertragung.



Labelbasierte Filterung an sicherem Netzübergang

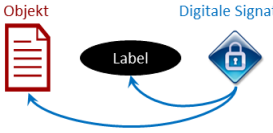
Security Label können darüber hinaus auch für die Zugriffskontrolle innerhalb von Sicherheitsdomänen verwendet werden („Darf eine Person ein Datenobjekt lesen?“) und als Grundlage für die elektronische VS-Bearbeitung und Nachweisführung.

Die **Speicherung** der Security Label erfolgt in der Regel getrennt vom Datenobjekt („detached“), z.B. als eigene Datei. In manchen Anwendungsfällen bietet es sich an, das Security Label direkt in das Datenobjekt einzubinden („embedded label“). Es ist auch möglich, dass das Datenobjekt in das Security Label integriert wird („enveloping label“).



Bindungsarten zw. Security Label und Datenobjekt

Nach dem Labeln können weder das Security Label noch das Datenobjekt unbemerkt verändert werden. Beispielsweise könnte ein Angreifer versuchen, den Geheimhaltungsgrad herabzusetzen, um ein Datenobjekt durch ein Sicherheitsgateway schleusen zu können. Er könnte ebenfalls versuchen, nachträglich geheime Informationen in ein „VS-NfD“ eingestuftes Datenobjekt einzufügen.
Um dies zu verhindern, werden Security Label mit Hilfe **digitaler Signaturen** an das Datenobjekt gebunden. Die digitale Signatur bezieht sich sowohl auf den Inhalt des Datenobjekts als auch auf das Security Label.



Sichere Bindung zw. Datenobjekten und digitaler Signatur

Änderungen am Security Label oder am Datenobjekt machen die digitale Signatur ungültig und können daher entdeckt werden.

SDoT
SecureDomainTransition

infodas
COLOGNE IT SOLUTIONS & SERVICES

Labelling mit SDoT® 6.0

Elektronische Kennzeichnung von Datenobjekten als Grundlage für die Filterung an Sicheren Netzübergängen - Realisierung

Das Sicherheitsgateway **SDoT**® 6.0 verfügt über folgende Labelling-Funktionalitäten

- **Manuelles Labelling**
  Anwender können mit dem **SDoT**®-Viewer die VS-Einstufung von Dokumenten bewerten und ein passendes Security Label für das Dokument erzeugen.

- **Automatisches Labelling**
  Für stark strukturierte Daten im XML-, ADEXP-, ASTERIX- oder FSD-Format kann auf dem **SDoT**®-Sicherheitsfilter ein Regelwerk hinterlegt werden, anhand dessen der Sicherheitsfilter automatisiert die VS-Einstufung einer Nachricht feststellen und ein entsprechendes Security Label selbst erzeugen kann.

- **Label-Verifikation**
  Der **SDoT**®-Sicherheitsfilter am Netzübergang prüft die Security Label der von HIGH empfangenen Nachrichten und vergleicht die enthaltene VS-Einstufung mit der VS-Einstufung des LOW Netzes. Fehlerhafte oder fehlende Security Label führen zur Ablehnung der Nachricht.

Als Datenformat für die Security Label nutzt **SDoT**® 6.0 die von der NATO entwickelte Syntax für „XML Security Label“.

Die Werte (z.B. „GEHEIM“ oder „SECRET“, „KRYPTO-SICHERHEIT“ oder „RELEASABLE TO ISAF“) und die zulässigen Wertekombinationen lassen sich in **SDoT**® 6.0 frei konfigurieren.

Die Security Label werden durch eine digitale Signatur im XML Format an das Datenobjekt gebunden („starke Bindung“).

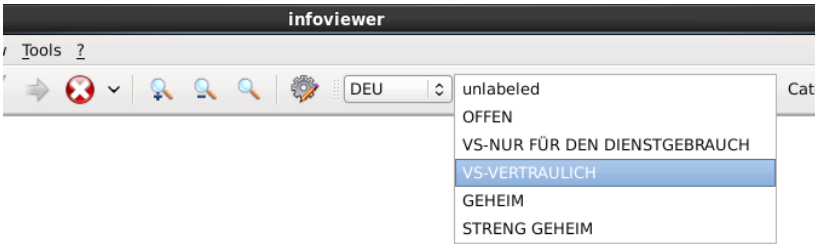
Die NATO hat in einer dreijährigen Labelling-Studie* (2007 – 2010) einen Entwurf für Security Labels spezifiziert, der auf XML beruht. Vorteile dieser zur Standardisierung vorgesehenen XML Security Labels gegenüber anderen Formaten:

- Gute Interoperabilität mit anderen XML-basierten Technologien (z.B. Web-Services, Office-Dateiformate)
- Sehr flexibler Bindungsmechanismus (ermöglicht z.B. die Erweiterung des Security Labels um weitere Inhalte)
- Zu erwartende NATO Standardisierung (sichert Interoperabilität mit anderen Bündnispartnern)

Derzeit werden auf Basis dieser Studie STANAGs erstellt (4774 und 4778). **SDoT**® wird mit diesen STANAGs kompatibel sein.

SDoT® hat im Rahmen der CWID 2009 seine Interoperabilität mit den NATO Vorgaben bewiesen.

*) [NATO RTO IST-068/RTG-031 Task Group on „XML in Cross-Domain Security Solutions“]



Beispiel für manuelles Labelling mit dem **SDoT**®-Viewer

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