Risiken bei der Übermittlung von Geschäftsdokumenten

Swisscom@swissDIGIN-Forum, 21. Juni 2017, Basel

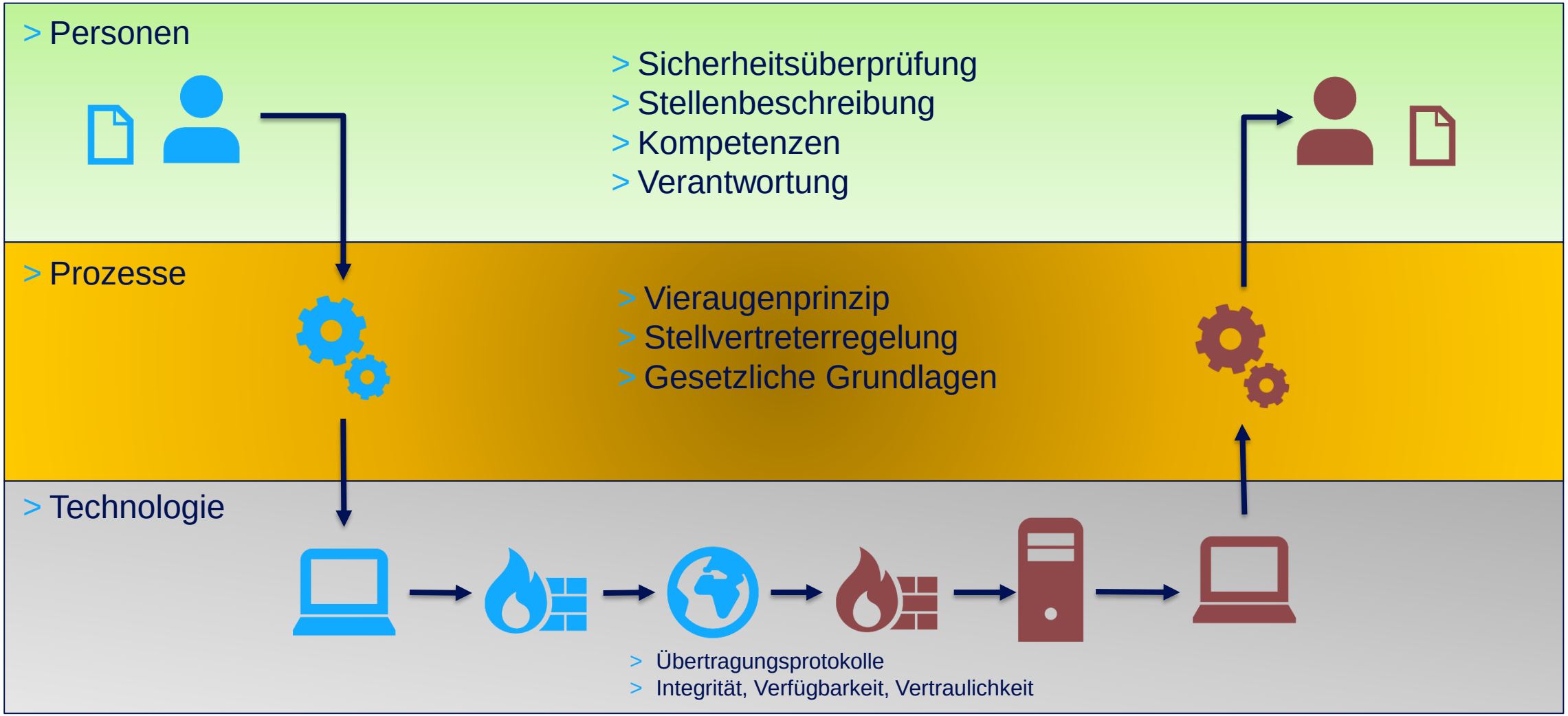
swisscom

Die technische Sicht

Dominique Brack
Senior Security Consultant, Swisscom

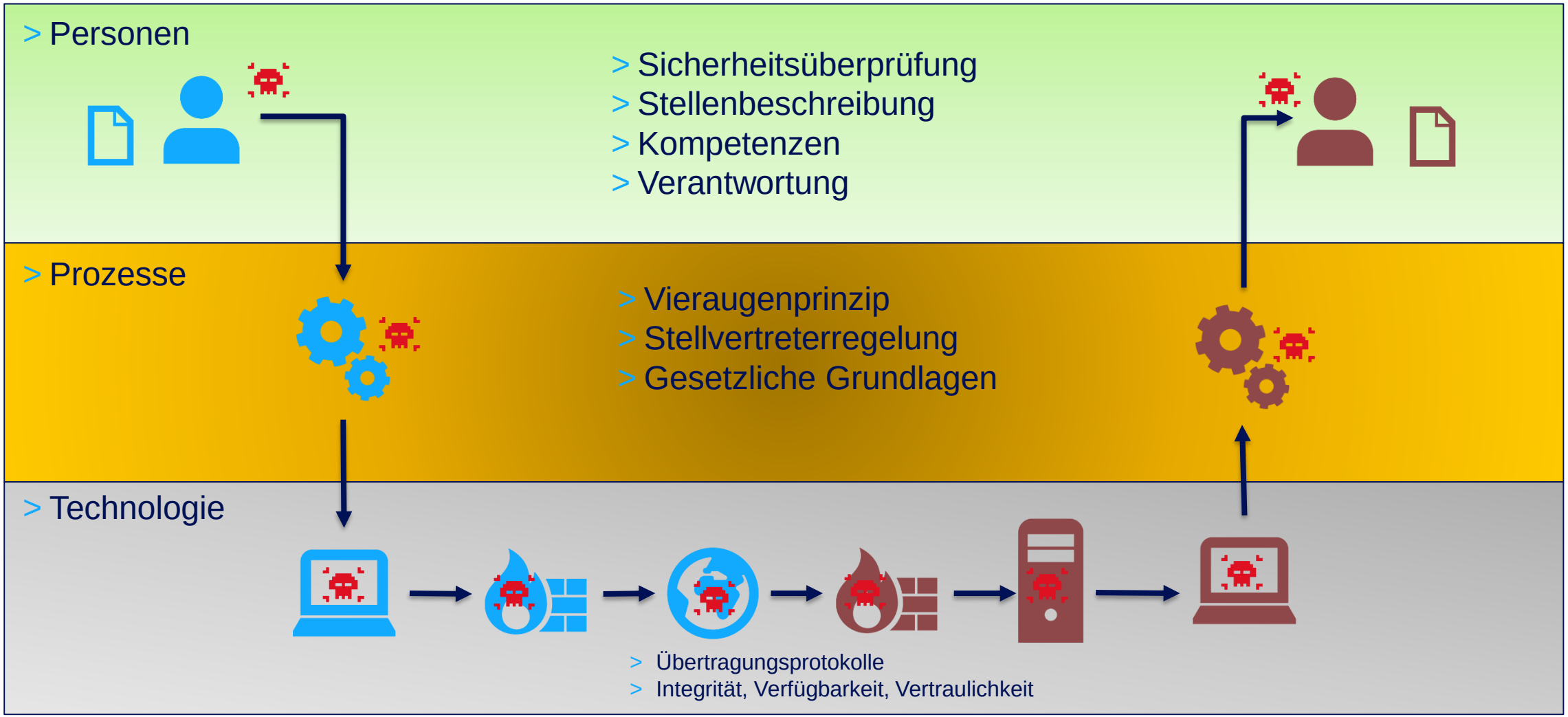
swisscom

Sicherheit ist ein Prozess



swisscom

Die Hackersicht



swisscom

Die Risiken

- Person
  - Insider Risiko
  - Falsche Rechnungen
  - Falsche Begünstigte
  - 2-fach Rechnungen
  - Keine Rechnung
  - Überschr. v. Limiten
  - Geldwäscherei
  - Menschliche Fehler

- Prozesse
  - Gesetzl. Grundlage fehlt
  - Kein 4-Augenprinzip
  - Keine Stellvertreterregelung
  - Falsche Berechtigungen
  - Nicht Revisionssicher
  - Kein BCM und DR
  - Kein Sicherheitskonzept
  - Kein SLA (Outsourcing oder Infrastruktur)
  - Verantwortung unklar
  - Keine Risikoanalyse
  - Keine aktives Monitoring der allg. Bedrohungslage

- Technologie
  - Keine Persönlichen Accounts
  - Keine Zertifikate
  - Keine Security Updates
  - Keine Verfügbarkeit
  - Veraltete Kom. Protokolle
  - Malwareschutz nicht aktuell
  - Antivirenschutz nicht aktuell
  - Ungenügende Segregation
  - Keine Redundanz
  - Shellshock, Heartbleed, Poodle
  - Ransomware Befall



swisscom

Übersicht der Protokolle

AS 2

HTTP(s)

(s)FTP

SMTP / E-Mail

X.400

General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

> Organisationen ohne Niederlassung in der EU

Fähigkeit, die laufende Vertraulichkeit, Integrität, und Verfügbarkeit zu gewährleisten

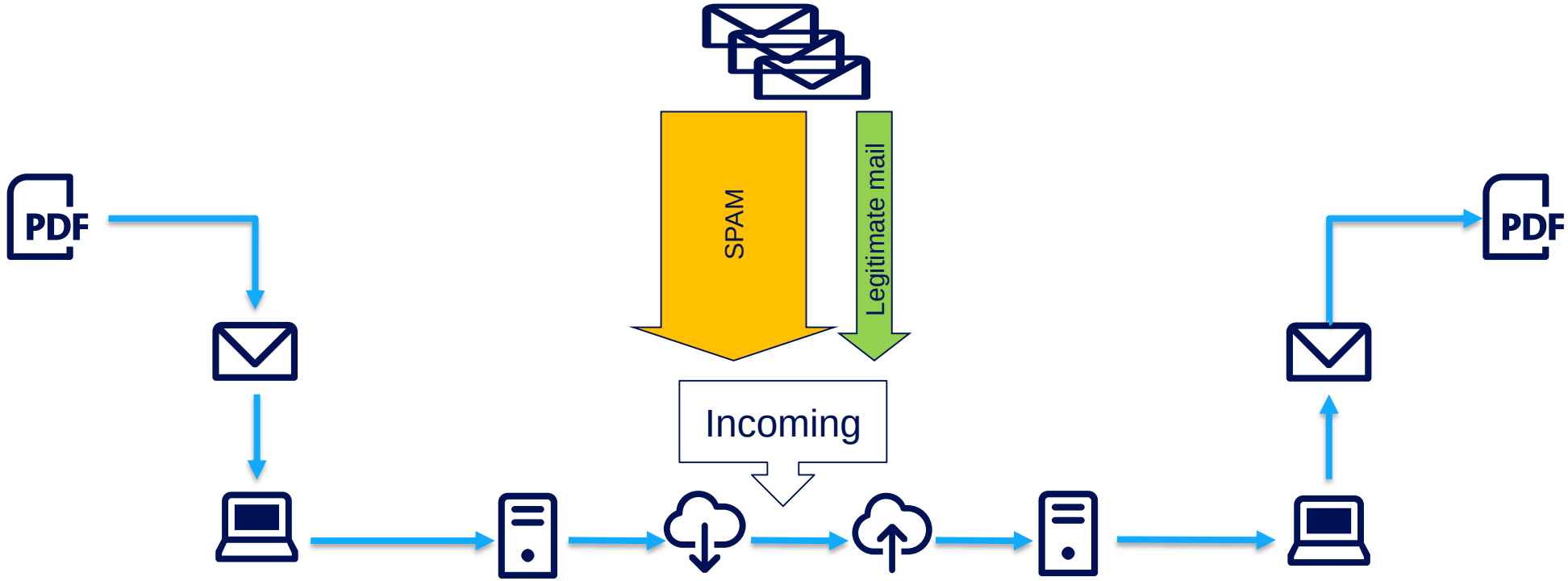
Sicherheitsvorfall… Mitteilung ist unverzüglich oder spätestens nach 72 Stunden

Pseudonymisierung und Verschlüsselung personenbezogener Daten

10 000 000 € oder 2 % seines gesamten weltweiten Jahresumsatzes oder bis zu 4%

swisscom

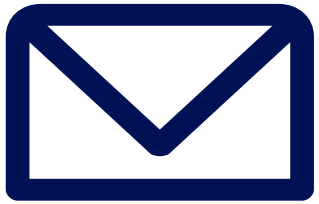
Email Prozess



> eMail black list/ white list
> Antivirus
> Antispam
> Antimalware
> Quarantine
> SPF
> Phishing/ Spearphishing

swisscom

Email



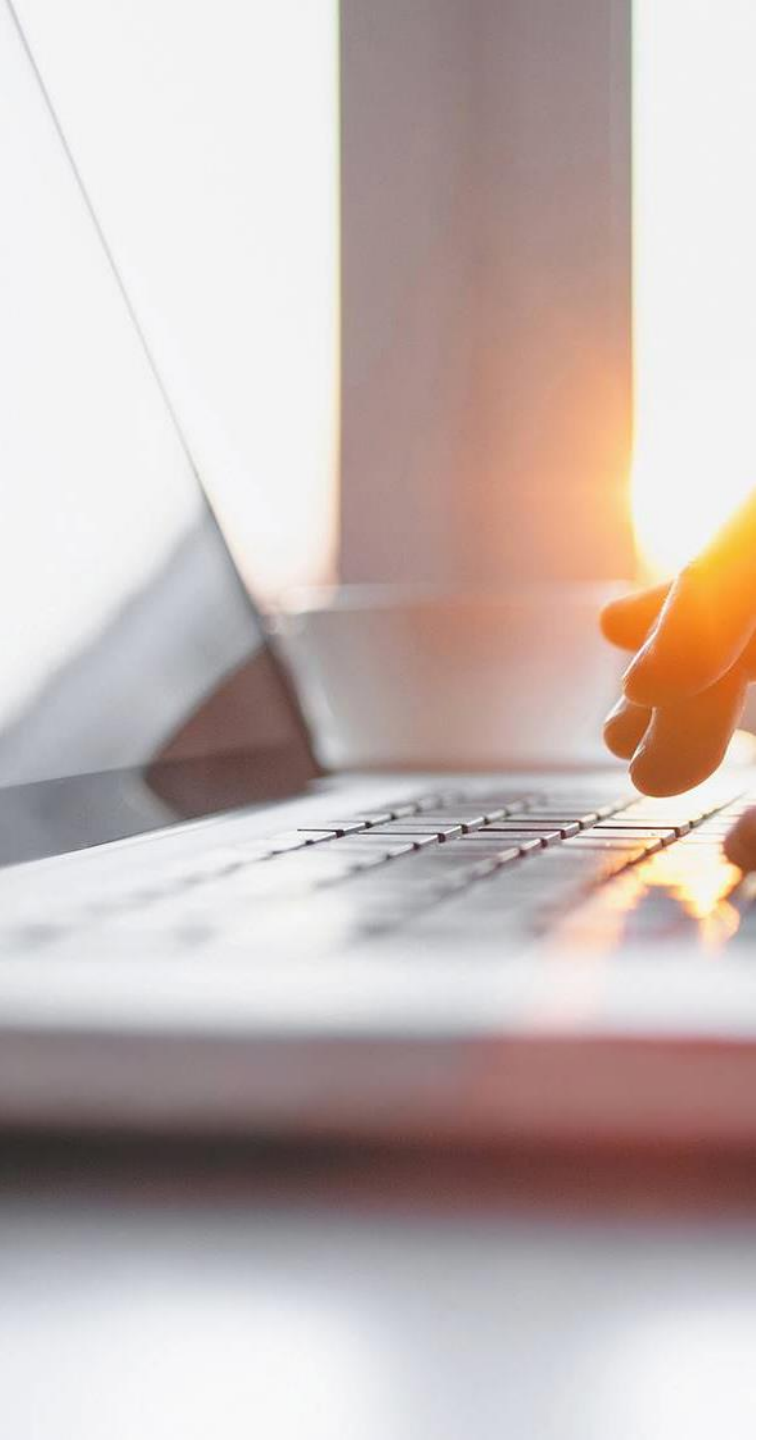
Email Typ	Integritätsnachweis, Herkunftsnachweis	Verschlüsselung	Authentisierung	Beziehungsvertraulichkeit	Lesebestätigung	Sendebestätigung, Lesequittung	eGov Behörde nach CH
Standard eMail	✗	✗	✗	✗	✗	✗	✗
Signiertes email	✓	✗	✗	✗	✗	✗	✗
Verschlüsseltes eMail	✓	✓	✗	✗	✗	✗	✗
ZertDS eMail	✓	✓	✓	✓	✓	✓	✓

swisscom

Aus Prozess-Sicht

Patric Knus
Sales Executive Conextrade, Swisscom

swisscom



Klassische Ziele der Informationssicherheit

Integrität	Authentizität	Verfügbarkeit
Korrektheit und Unversehrtheit der Daten	Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit	Anforderungen zu Zeitrahmen und Qualität

Der elektronische Geschäftsverkehr EGV: Keine Pflicht zur digitalen Signatur

Bei übermittelten und aufbewahrten Daten, die für den Vorsteuerabzug, die Steuererhebung oder den Steuerbezug relevant sind, muss unabhängig davon, ob sie auf Papier oder elektronisch vorliegen, der Nachweis des Ursprungs und der Unverändertheit erbracht werden. Bei elektronischen Daten ist dieser Nachweis insbesondere dann erbracht, wenn die elektronischen Daten digital signiert sind. Eine digitale Signatur bietet den besten Schutz vor nicht feststellbaren Veränderungen. Aufgrund des Grundsatzes der Beweismittelfreiheit kann der Nachweis des Ursprungs und der Unverändertheit aber auch dann als erbracht angenommen werden, wenn die Grundsätze ordnungsmässiger Buchführung nach Artikel 957a OR eingehalten sind. Die Papierrechnung und die elektronische Rechnung sind gleichgestellt, denn die Grundsätze ordnungsmässiger Buchführung gelten für alle Arten von Buchungsbelegen.

Quelle: https://www.estv.admin.ch/estv/de/home/mehrwertsteuer/fachinformationen/elektronischer-geschaeftsverkehr.html

swisscom

Der elektronische Geschäftsverkehr EGV: Keine Pflicht zur digitalen Signatur

Bei übermittelten und aufbewahrten Daten, die für den Vorsteuerabzug, die Steuererhebung oder den Steuerbezug relevant sind, muss unabhängig davon, ob sie auf Papier oder elektronisch vorliegen, der Nachweis des Ursprungs und der Unverändertheit erbracht werden. Bei elektronischen Daten ist dieser Nachweis insbesondere dann erbracht, wenn die elektronischen Daten digital signiert sind. Eine digitale Signatur bietet den besten Schutz vor nicht feststellbaren Veränderungen. Aufgrund des Grundsatzes der Beweismittelfreiheit kann der Nachweis des Ursprungs und der Unverändertheit aber auch dann als erbracht angenommen werden, wenn die Grundsätze ordnungsmässiger Buchführung nach Artikel 957a OR eingehalten sind. Die Papierrechnung und die elektronische Rechnung sind gleichgestellt, denn die Grundsätze ordnungsmässiger Buchführung gelten für alle Arten von Buchungsbelegen.

Quelle: https://www.estv.admin.ch/estv/de/home/mehrwertsteuer/fachinformationen/elektronischer-geschaeftsverkehr.html

swisscom

Stand gestern

Rechnungssteller

Sichere Verbindung zum Provider.

Provider

Anbringen der Signatur.

Rechnungsempfänger

Sichere Verbindung zum Provider.

Signatur und gesicherte Übermittlung:
Authentizität und Integrität der Daten ist garantiert

swisscom

Stand morgen

Rechnungssteller

Ungesicherte Verbindung zum Handelspartner.

Rechnungsempfänger

Ungesicherte Verbindung zum Handelspartner.

Keine Signatur und ungesicherte Übermittlung:
Authentizität und Integrität der Daten ist technisch NICHT garantiert

swisscom

Änderungen und entstehende Tendenzen

Veränderung	Konsequenz
Wegfall der Signaturpflicht	Prozessvereinfachung
Zunahme von elektronischen Rechnungen per Mail	Entwicklung neuer Risiken: Spam, Spoofing, Data Privacy, Data Leaking, etc..
Gleichstellung von physischer und elektronischer Rechnung	Eigenverantwortung der Handelspartner steigt

swisscom

Aus Sicht von Conextrade…

Integrität

Eine gesicherte Übermittlung schützt die Integrität von Daten

Eine digitale Signatur bietet weiterhin den besten Schutz Veränderungen

Implementierung neuer Technologien / Methoden (z.B. Blockchain)

Authentizität

Die Relevanz von sicheren Verbindungen nimmt zu

Neue Services unterstützen bei ungesicherter Übermittlung (z.B. White Listing bei E-Mail)

Der Provider muss helfen, die Authentizität sicherzustellen

Verfügbarkeit

Zuverlässigkeit der E-Mail als Übertragungsmedium ist nicht gewährleistet

Sicherstellung der Rechnungszustellung

Status der Rechnungsbearbeitung ist wünschenswert

swisscom

Fazit

- Freiheit bedeutet nicht Einfachheit!
- Der Weg über Provider bedeutet nicht nur Rechtssicherheit, sondern auch Prozessvereinfachung
- Strukturierte Übertragung erspart unstrukturierte Kommunikation

Vielen Dank!

Basel, 21. Juni 2017

swisscom