E-Government Gesetz Sachsen

Dierk Schlosshan, eureos gmbh

10. März 2016

eureos

Gliederung

I. E-Government-Gesetz Sachsen – Überblick

II. Einzelpflichten und Optionen

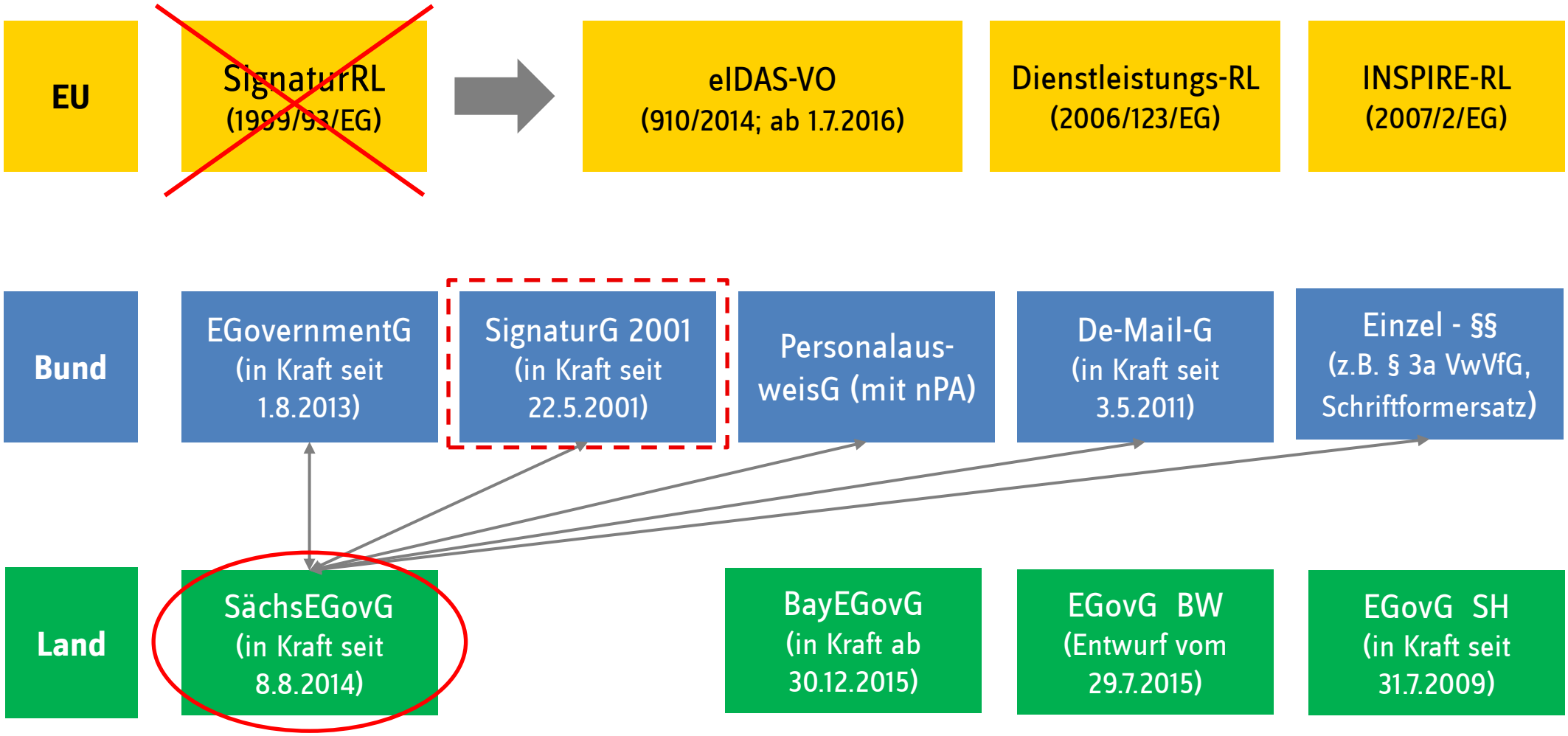
1. Elektronische Kommunikation und Verschlüsselung

- Pause -

2. Zugang für schriftformersetzende Dokumente
3. Datenschutz
4. Informationssicherheit
5. Basiskomponenten

I. SächsEGovG-Überblick

Rechtsgrundlagen E-Government



Anwendungsbereich

2 Gruppen von Adressaten

- Landesbehörden (Art. 82 Abs. 1, Art. 83 SächsVerf, vgl. Sächsisches Verwaltungsorganisationsgesetz)
- Träger der Selbstverwaltung (TdS, Art. 82 Abs. 2 S. 1 SächsVerf)
  - kommunale TdS (Gemeinde, Landkreise, Gemeindeverbände inkl. Eigenbetriebe)
  - Nicht-kommunale TdS (öffentlich-rechtliche Körperschaften, Anstalten, Stiftungen)

→ Nicht / eingeschränkt:

- MDR (§ 1)
- Beliehene:
  - Unabhängig von Beleihendem nur Regelungen für TdS anwendbar
  - abgeschwächt (z.B. elektr. Kommunikation nur, soweit „erforderlich“, § 2 Abs. 1 S 2)
- Justiz: Nur Justizverwaltung (§ 1 Abs. 3)
- Kommunale Gesellschaften? (-), wenn kein öffentlich-rechtliches Verwaltungshandeln (insbesondere bei Handeln in Form des Verwaltungsprivatrechts)

Anwendungsbereich

Sächsisches EGovG oder Bundes EGovG?

§ 1 Abs. 1 SächsEGovG:

„Dieses Gesetz regelt die elektronisch unterstützte **öffentlich-rechtliche Verwaltungstätigkeit der Behörden des Freistaates Sachsen sowie der** seiner Aufsicht unterliegenden Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts **(Träger der Selbstverwaltung).** Auf Beliehene finden die Vorschriften dieses Gesetzes für die Träger der Selbstverwaltung Anwendung..“

§ 1 Abs. 2 BEGovG:

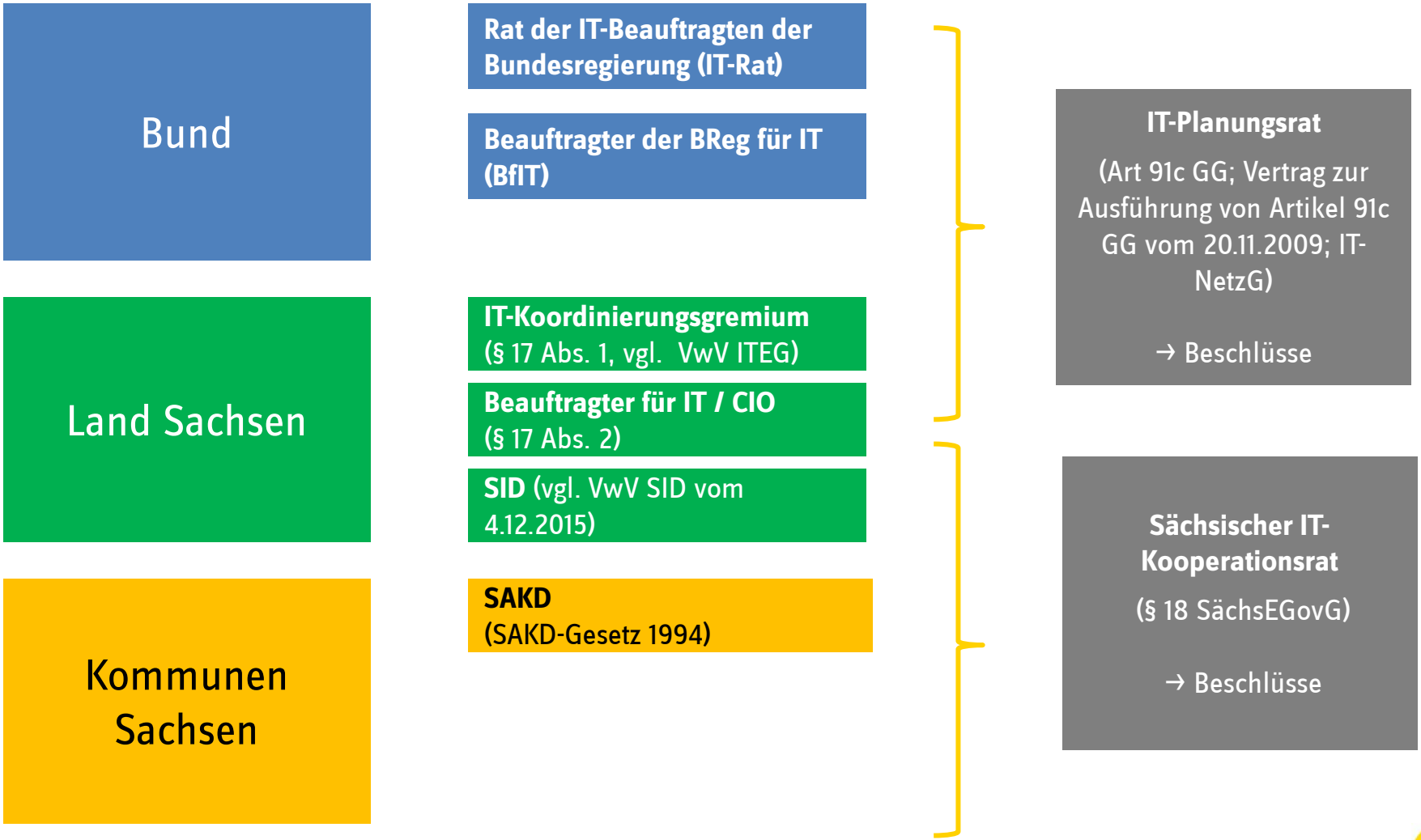
„Dieses Gesetz gilt auch für die **öffentlich-rechtliche Verwaltungstätigkeit der Behörden der Länder, der Gemeinden und Gemeindeverbände** und der sonstigen der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts, **wenn sie Bundesrecht ausführen.**“

Gesetze	Vollzug				
	Bund	Länder			
Bundesrecht	Ausnahme (vgl. Art. 86ff GG)	**als eigene Angelegenheit** - "Bundesaufsichtsverwaltung" (Art. 84 GG) · Regel (Art. 30, 83 ff GG) · (Nur) Rechtsaufsicht des Bundes	Unmittelbare Landesverwaltung - **Landesbehörden**	Mittelbare Landesverwaltung - u.a. **Gemeinden**	→ BEGovG
		Im Auftrag des Bundes - „Bundesauftragsverwaltung" (Art. 85 GG) · Abschließende Aufzählung · Rechts- und Fachaufsicht des Bundes			
Landesrecht	--	Regel (grundsätzliche Zuständigkeit der Länder, Art. 30, 83 ff GG)	Unmittelbare Landesverwaltung - **Landesbehörden**	Mittelbare Landesverwaltung - u.a. **Gemeinden**	→ SächsEGovG
Gemeinderecht	--	--	--	Regel (Angelegenheiten der örtlichen Gemeinschaft, Art. 28 Abs. 2 GG, Art. 82 Abs. 2 Satz 2 SächsVerf)	→ SächsEGovG

Gesetz-Aufbau und Struktur

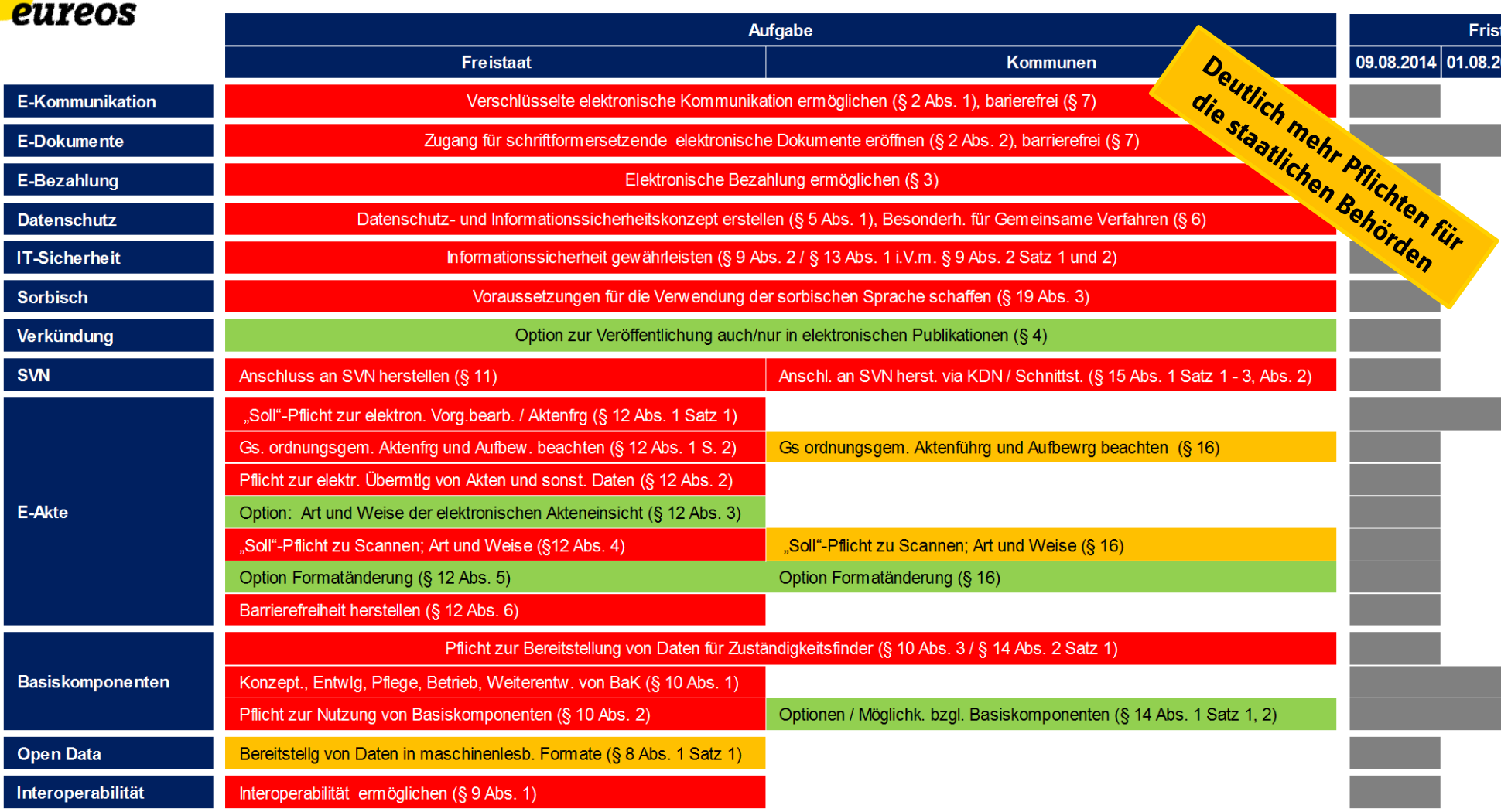
- 4 Arten von Regelungen:
  - Pflichten
  - Optionen, Möglichkeiten
  - „Soweit“-Regelungen
  - Organisatorische Regelungen
- Adressaten (Freistaat bzw. Träger der Selbstverwaltung) unterschiedlich verpflichtet
- 3 Umsetzungs-Fristen
- z.T. Vorbehalte (Haushalt, wichtiger Grund)
- VO-Ermächtigungen
  - § 8 Abs. 3 - Open Data
  - § 10 Abs. 4 Satz 1, 2 - Basiskomponenten-Liste und -nutzungsfristen (für den FS)
  - § 10 Abs. 4 Satz 3, 4 - Basiskomponenten Ausgestaltung
  - § 15 Abs. 2 Satz 1 - Schnittstelle zu SVN, Alternative zu KDN
  - § 20 Abs. 1 - Experimentierklausel, Ausnahmen von VwVf- und VwZ-Kosten

Organisatorische Regelungen IT



Sächsisches E-Government-Gesetz - Überblick

Dierk Schlosshan, 27.8.2015



	Aufgabe		Frist			Vbh
	Freistaat	Kommunen	09.08.2014	01.08.2016	01.08.2018	
E-Kommunikation	Verschlüsselte elektronische Kommunikation ermöglichen (§ 2 Abs. 1), barierefrei (§ 7)					
E-Dokumente	Zugang für schriftformersetzende elektronische Dokumente eröffnen (§ 2 Abs. 2), barrierefrei (§ 7)					1
E-Bezahlung	Elektronische Bezahlung ermöglichen (§ 3)					
Datenschutz	Datenschutz- und Informationssicherheitskonzept erstellen (§ 5 Abs. 1), Besonderh. für Gemeinsame Verfahren (§ 6)					
IT-Sicherheit	Informationssicherheit gewährleisten (§ 9 Abs. 2 / § 13 Abs. 1 i.V.m. § 9 Abs. 2 Satz 1 und 2)					
Sorbisch	Voraussetzungen für die Verwendung der sorbischen Sprache schaffen (§ 19 Abs. 3)					
Verkündung	Option zur Veröffentlichung auch/nur in elektronischen Publikationen (§ 4)					
SVN	Anschluss an SVN herstellen (§ 11)	Anschl. an SVN herst. via KDN / Schnittst. (§ 15 Abs. 1 Satz 1 - 3, Abs. 2)				
E-Akte	„Soll"-Pflicht zur elektron. Vorg.bearb. / Aktenfrg (§ 12 Abs. 1 Satz 1)					2
	Gs. ordnungsgem. Aktenfrg und Aufbew. beachten (§ 12 Abs. 1 S. 2)	Gs ordnungsgem. Aktenführg und Aufbewrg beachten (§ 16)				
	Pflicht zur elektr. Übermtlg von Akten und sonst. Daten (§ 12 Abs. 2)					3
	Option: Art und Weise der elektronischen Akteneinsicht (§ 12 Abs. 3)					
	„Soll"-Pflicht zu Scannen; Art und Weise (§12 Abs. 4)	„Soll"-Pflicht zu Scannen; Art und Weise (§ 16)				
	Option Formatänderung (§ 12 Abs. 5)	Option Formatänderung (§ 16)				
	Barrierefreiheit herstellen (§ 12 Abs. 6)					
Basiskomponenten	Pflicht zur Bereitstellung von Daten für Zuständigkeitsfinder (§ 10 Abs. 3 / § 14 Abs. 2 Satz 1)					
	Konzept., Entwlg, Pflege, Betrieb, Weiterentw. von BaK (§ 10 Abs. 1)					4
	Pflicht zur Nutzung von Basiskomponenten (§ 10 Abs. 2)	Optionen / Möglichk. bzgl. Basiskomponenten (§ 14 Abs. 1 Satz 1, 2)				
Open Data	Bereitstellg von Daten in maschinenlesb. Formate (§ 8 Abs. 1 Satz 1)					
Interoperabilität	Interoperabilität ermöglichen (§ 9 Abs. 1)					

Vorbehalte

1. wichtiger Grund + HH-Mittel, § 2 Abs. 2
2. HH-Mittel, § 12 Abs. 1 Satz 1
3. wichtiger Grund + HH-Mittel, § 12 Abs. 2
4. Rechts-VO; HH-Mittel, § 10 Abs. 4 S. 1

Legende

- Pflicht
- "Soweit"-Pflicht
- Option, Möglichkeit

Sächsisches E-Government-Gesetz - Pflichten/Optionen für die Träger der Selbstverwaltung

Dierk Schlosshan, 27.8.2015

		Aufgabe	Frist		
		Kommunen	09.08.2014	01.08.2016	01.08.2018
1	E-Kommunikation	Verschlüsselte elektronische Kommunikation ermöglichen (§ 2 Abs. 1), barierefrei (§ 7)			
2	E-Dokumente	Zugang für schriftformersetzende elektronische Dokumente eröffnen (§ 2 Abs. 2), barrierefrei (§ 7) [1]			
	E-Bezahlung	Elektronische Bezahlung ermöglichen (§ 3)			
3	Datenschutz	Datenschutz- und Informationssicherheitskonzept erstellen (§ 5 Abs. 1)			
4	IT-Sicherheit	Informationssicherheit gewährleisten (§ 9 Abs. 2 / § 13 Abs. 1 i.V.m. § 9 Abs. 2 Satz 1 und 2)			
	Sorbisch	Voraussetzungen für die Verwendung der sorbischen Sprache schaffen (§ 19 Abs. 3)			
	Verkündung	Option zur Veröffentlichung auch/nur in elektronischen Publikationen (§ 4)			
	SVN	Anschl. an SVN herst. via KDN / Schnittst. (§ 15 Abs. 1 Satz 1 - 3, Abs. 2)			
	E-Akte	Gs ordnungsgem. Aktenführg und Aufbewrg beachten (§ 16)			
		„Soll"-Pflicht zu Scannen; Art und Weise (§ 16)			
		Option Formatänderung (§ 16)			
5	Basiskomponenten	Pflicht zur Bereitstellung von Daten für Zuständigkeitsfinder (§ 10 Abs. 3 / § 14 Abs. 2 Satz 1)			
		Optionen / Möglichk. bzgl. Basiskomponenten (§ 14 Abs. 1 Satz 1, 2)			

Pflicht
"Soweit"-Pflicht
Option, Möglichkeit

Anmerkungen

1 vorbehaltlich wichtiger Grund + HH-Mittel, § 2 Abs. 2

II. Einzelregelungen

1 E-Kommunikation und Verschlüsselung

E-Kommunikation u. Verschlüsselung

Rechtsgrundlage

Frist: 9.8.2014

§ 2 Abs. 1 SächsEGovG:

„Die staatlichen Behörden und die Träger der Selbstverwaltung müssen auch die **elektronische Kommunikation ermöglichen**. Beliehene sind von dieser Verpflichtung ausgenommen, soweit die elektronische Kommunikation für die ordnungsgemäße Wahrnehmung ihrer Verwaltungsaufgaben nicht erforderlich ist. **Für die elektronische Kommunikation sind Verschlüsselungs-verfahren anzubieten und grundsätzlich anzuwenden**."

§ 7 SächsEGovG

„Die staatlichen Behörden und die Träger der Selbst-verwaltung gestalten die elektronische Kommunikation …**schrittweise** so, dass sie auch von Menschen mit Behin-derungen grundsätzlich uneingeschränkt und barrierefrei nach § 3 …SächsIntegrG… genutzt werden können."

Frist: 1.7.2014

§ 2 Abs. 1 BEGovG:

„Jede Behörde ist verpflichtet, auch einen Zugang für die Übermittlung elektronischer Dokumente, auch soweit sie mit einer qualifizierten elektronischen Signatur versehen sind, zu eröffnen."

Minikommentar zum BEGovG, S. 12

Absatz 1 verpflichtet alle Behörden, neben den allgemein üblichen Zugängen zur Verwaltung … auch einen Zugang für die elektronische Kommunikation zu eröffnen.

E-Kommunikation u. Verschlüsselung

Rechtsgrundlage (Forts.)

Frist: 9.8.2014

§ 7 SächsEGovG

„Die staatlichen Behörden und die Träger der Selbstverwaltung gestalten die elektronische Kommunikation …**schrittweise** so, dass sie auch von Menschen mit Behinderungen grundsätzlich uneingeschränkt und barrierefrei nach § 3 …SächsIntegrG… genutzt werden können."

E-Kommunikation u. Verschlüsselung

Hintergrund

Angleichung an BEGovG zur Verhinderung unterschiedlicher Anforderungen an Kommunen

- Seit 1.7.2014 Pflicht zur elektronischen Kommunikation (wird in § 2 Abs. 1 BEGovG impliziert) bei Ausführung von Bundesrecht

- Adressat auch „…Gemeinden und Gemeindeverbände und … sonstige … der Aufsicht des Landes unterstehende juristische Personen des öffentlichen Rechts, wenn sie Bundesrecht ausführen…“ (§ 1 Abs. 2 BEGovG)

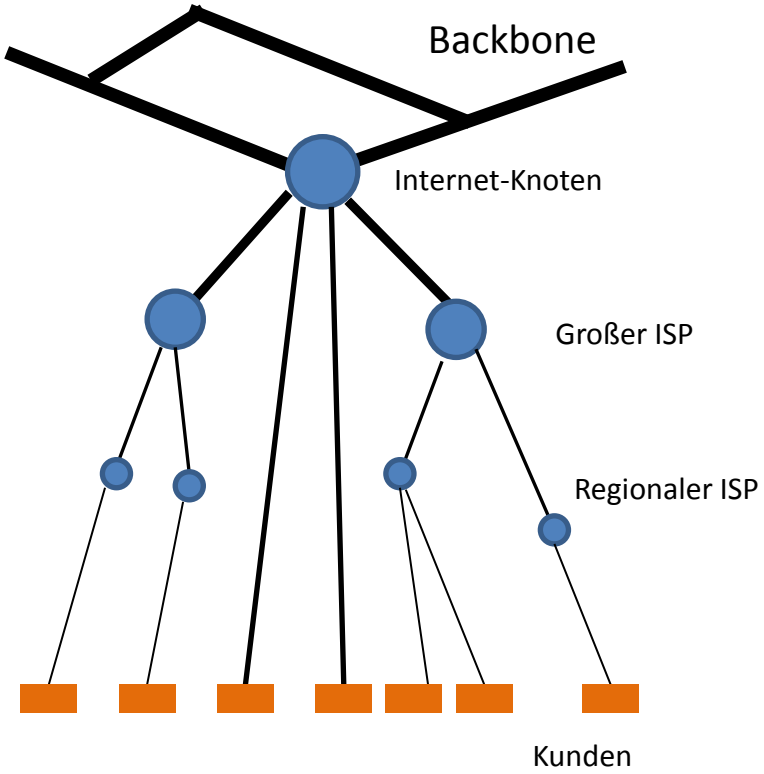
E-Kommunikation u. Verschlüsselung

Hintergrund (Forts.)

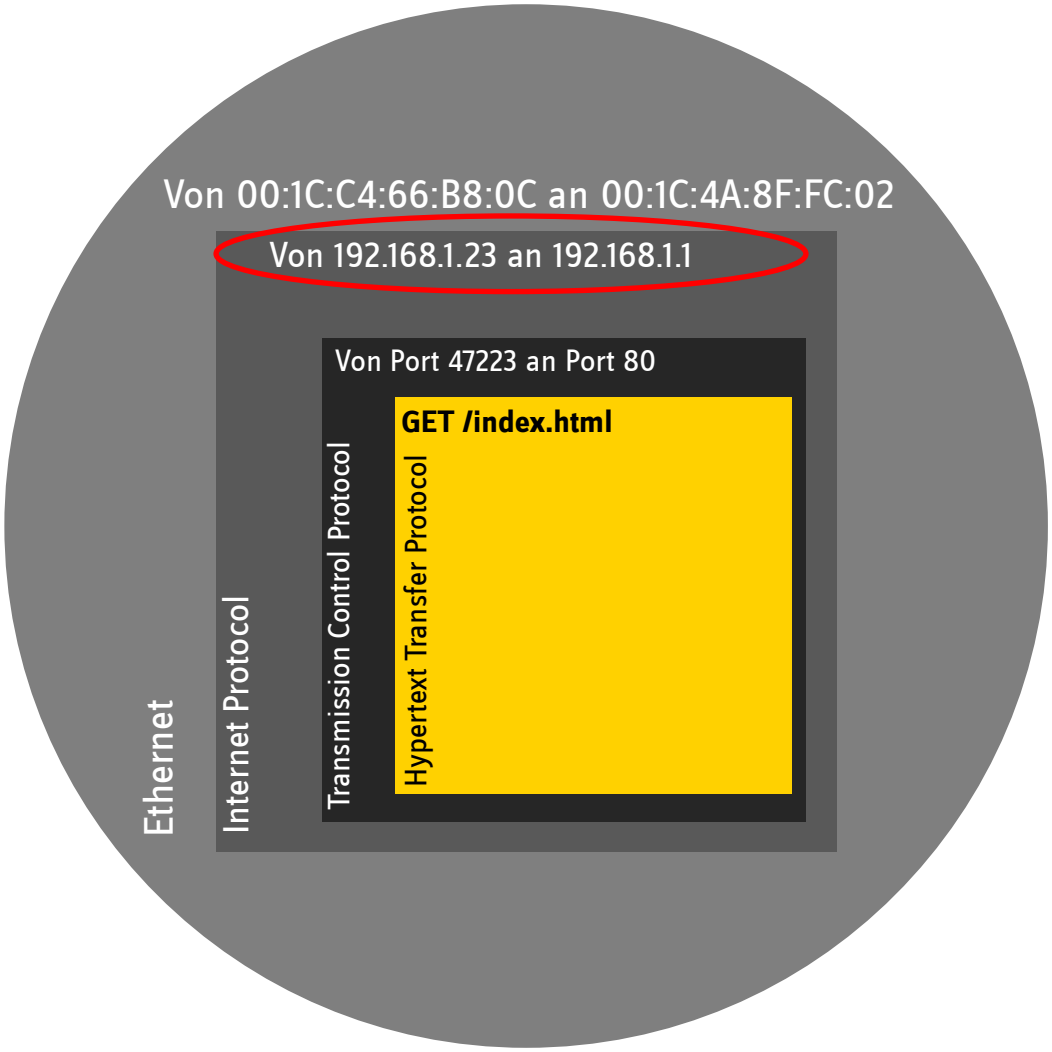
E-Mail versenden ist UNSICHER

E-Kommunikation u. Verschlüsselung

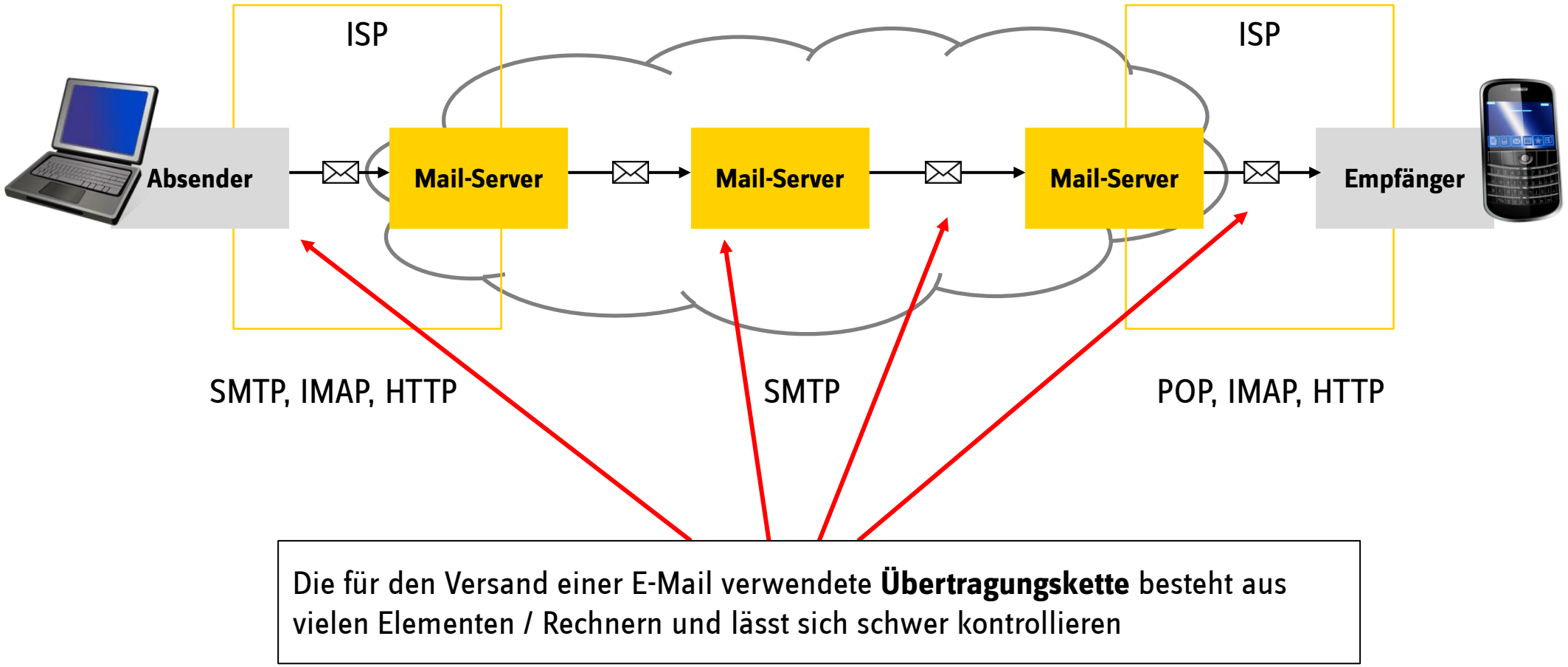
Hintergrund (Forts.)



Die **Infrastruktur** des Internet ist komplex und in weiten Teilen ungeschützt, so dass sich viele Möglichkeiten des „Anzapfens“ des Datenstroms bieten



Die Sprache des Internet, die sog. **Protokolle**, bedingt, dass auf den Datenpaketen die Verbindungsdaten im Klartext stehen. Dies kann zum gezielten Herausfiltern von E-Mail-Daten verwendet werden.



Die für den Versand einer E-Mail verwendete **Übertragungskette** besteht aus vielen Elementen / Rechnern und lässt sich schwer kontrollieren

E-Kommunikation u. Verschlüsselung

Hintergrund (Forts.)

Verschlüsselung schützt (zum Teil)

Schutzziel [1]	Erläuterung	Lösung
Verfügbarkeit	autorisierte Benutzer haben Zugriff auf Informationen und Systeme	ISMS (z.B. BSI IT-GS)
Authentizität	Gewissheit, dass Nachricht vom angegebenen Absender stammt	Elektronische Signatur
Integrität	Gewissheit, dass Inhalt der Nachricht vollständig und unverändert ist	
Vertraulichkeit - der Verbindungsdaten	Wer hat wann mit wem wie lange wo kommuniziert	Anonymisierungsdienste (VPN, TOR)
Vertraulichkeit - der Inhaltsdaten	Schutz vor Lesen von geheimen Informationen / pbD durch Dritte	Verschlüsselung

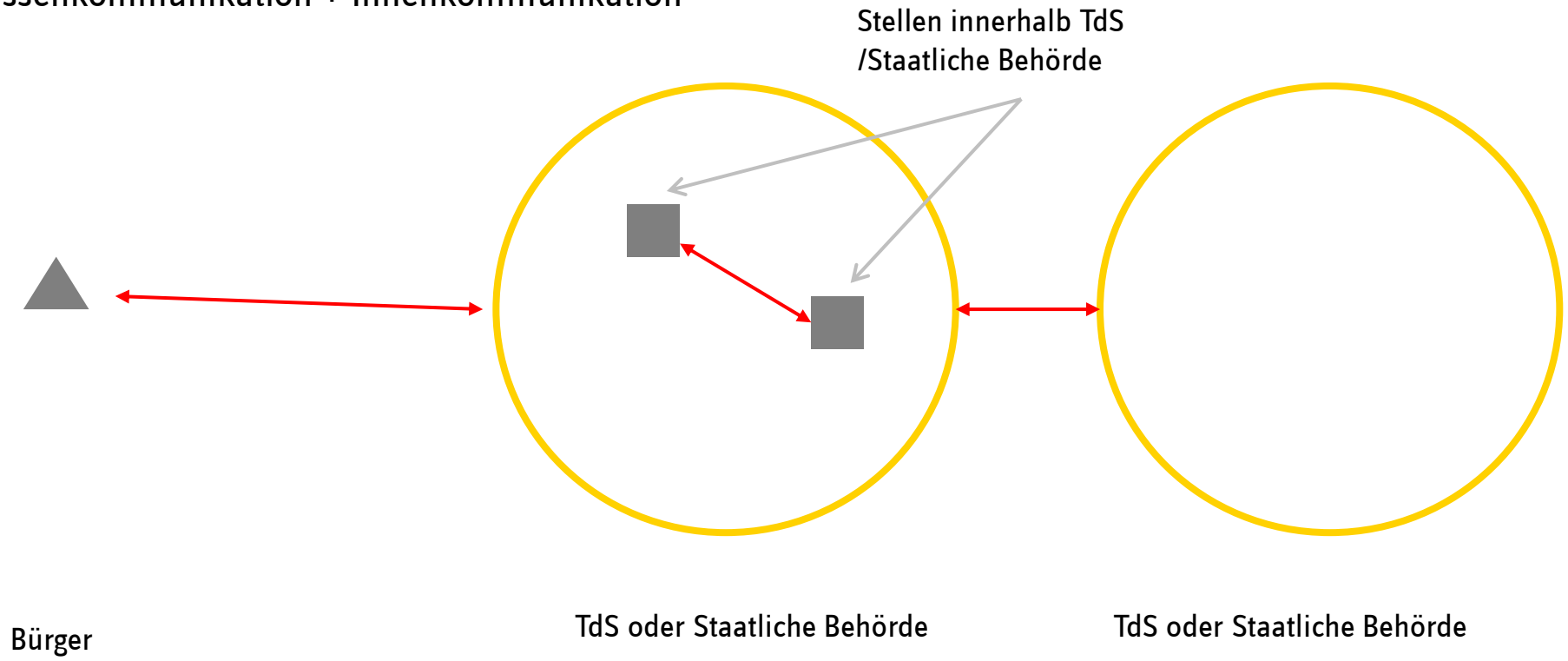
[1] vgl. § 9 Abs. 2 SächsDSG, § 8a Abs. 1 BSIG

Quelle: Verschlüsselung von E-Mails - Leitfaden, Datev/DsiN, 2013; BSI

E-Kommunikation u. Verschlüsselung

Sachlicher Anwendungsbereich

Aussenkommunikation + Innenkommunikation



Quelle: SMI, SächsEGovG, Handlungsleitfaden zur Umsetzung in kommunalen Behörden, Version 1.0, 6.2.2015, S. 13 ff.

E-Kommunikation u. Verschlüsselung

Inhalt

1. Elektronische Kommunikation ermöglichen

- Elektronische Kommunikation
  - „Unter der elektronischen Kommunikation versteht man das Senden und Empfangen von Nachrichten mittels elektronischer Medien.“ [1] → E-Mail-Postfach

- Ermöglichen
  - Schaffung der erforderlichen technischen und organisatorischen Voraussetzungen, um elektronische Kommunikationsvorgänge durchzuführen → Stand der Technik (empfohlen) [1]

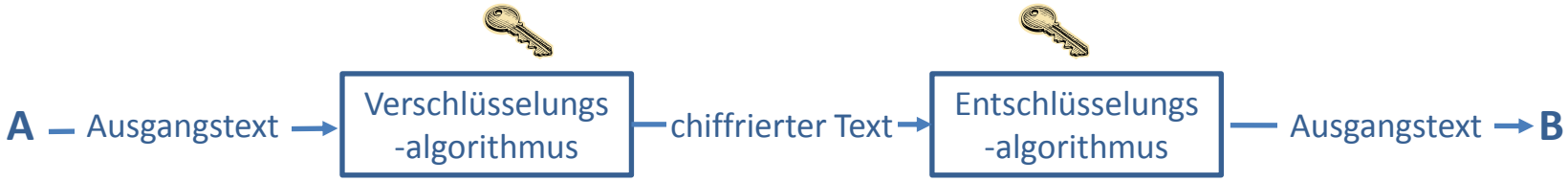
[1] SMI, SächsEGovG, Handlungsleitfaden zur Umsetzung in kommunalen Behörden, Version 1.0, 6.2.2015, S. 14

E-Kommunikation u. Verschlüsselung

Inhalt (Forts.)

2. Verschlüsselung anbieten und *grundsätzlich* auch anwenden

- Verschlüsselung:
  - „…das Einsetzen eines Verfahrens zum Schutz der Daten vor unbefugter Einsichtnahme oder Veränderung, in dem diese mittels eines entsprechenden Algorithmus in eine nur für den Berechtigten erschließbare Form gebracht werden…“ [1]



[1] SMI, SächsEGovG, Handlungsleitfaden zur Umsetzung in kommunalen Behörden, Version 1.0, 6.2.2015, S. 14

E-Kommunikation u. Verschlüsselung

Exkurs: Verschlüsselung 1/5

Überblick

1. Verfahren (Wie?)	a) Symetrisch – **ein** Schlüssel (zum Ver- und Ent-schlüsseln)	**oder / und**[1]	b) Asymetrisch – **zwei** Schlüssel (je 1 zum Ver- und Entschlüsseln)
2. Gegenstand (Was?)	a) Transport	**oder / und**	b) Inhalte

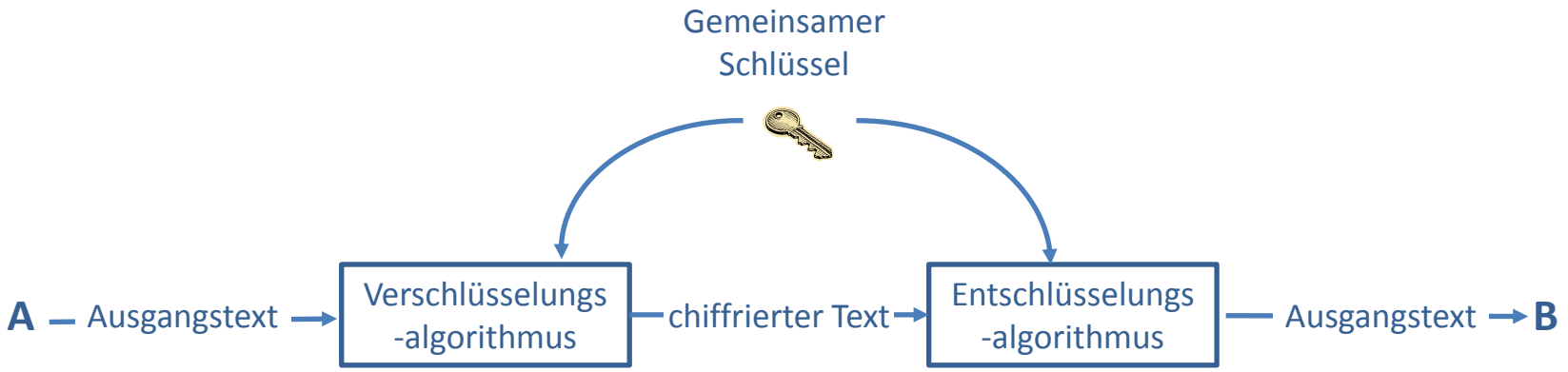
[1] Hybride Verschlüsselung der Session mit symetrischem Schlüssel; nur dieser wird asymetrisch verschlüsselt

Quelle: Institut für Informatik der Universität Potsdam

E-Kommunikation u. Verschlüsselung

Exkurs: Verschlüsselung 2/5

1. Verschlüsselungsverfahren: a) Symmetrisch



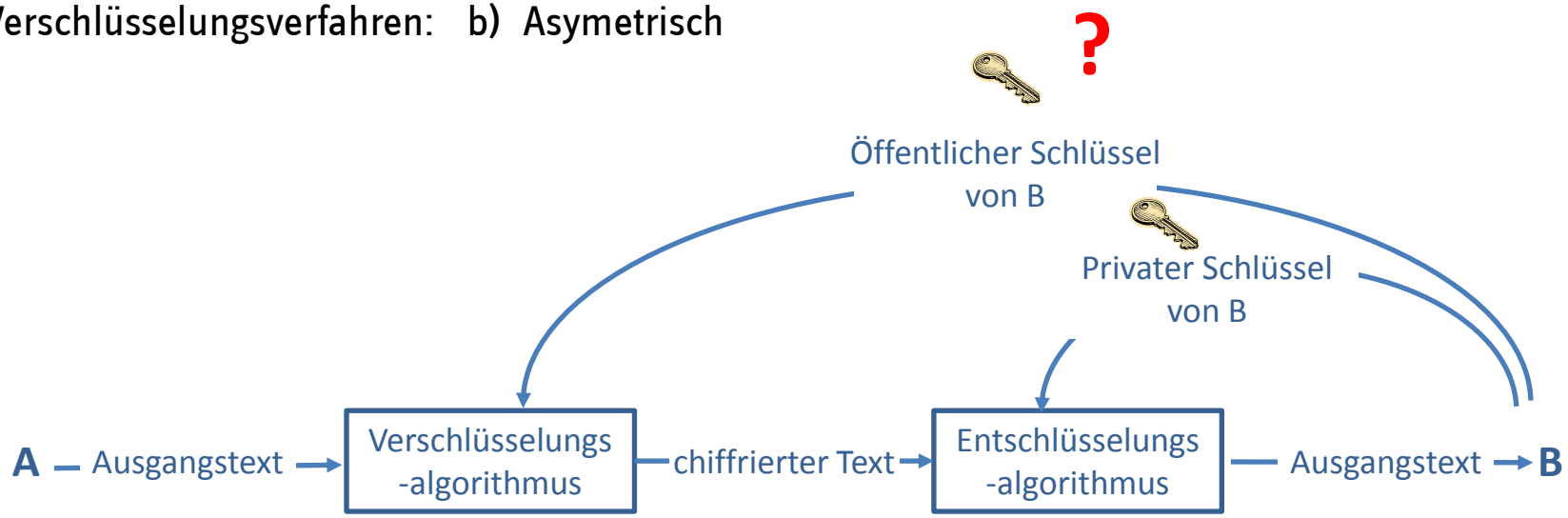
Erläuterung	Vor- und Nachteile
Beide K- Partner besitzen denselben Schlüssel (zum Ver- und Entschlüsseln) Beispiel: MS-Office, Zip	**(-) Schlüssel muss sicher ausgetauscht werden** (z.B. Kurier, Post) (+) Schnell

Quelle: Institut für Informatik der Universität Potsdam

E-Kommunikation u. Verschlüsselung

Exkurs: Verschlüsselung 3/5

1. Verschlüsselungsverfahren: b) Asymetrisch



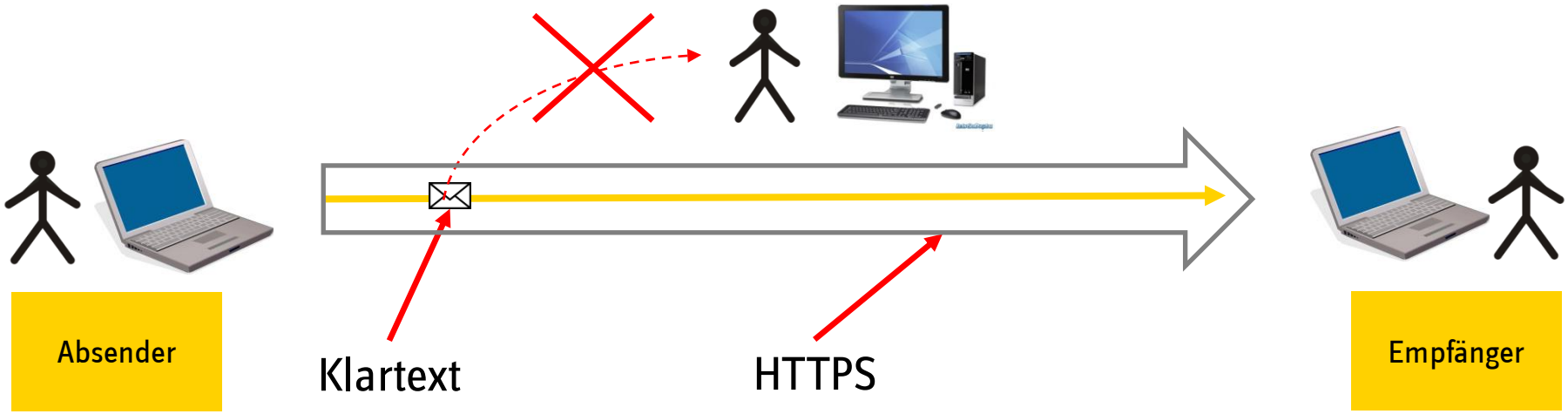
Erläuterung	Vor- und Nachteile
Empfänger B generiert Schlüsselpaar: Öffentlicher Schlüssel *von B* dient zum Verschlüsseln von Nachrichten an B, privater zum Entschlüsseln. Beispiel: RSA	(+) Öffentlicher Schlüssel offen verteilbar **(-) Risiko Fälschung öffentlicher Schlüssel p** **Authentifizierung des Schlüssels** notwendig (-) Langsam

Quelle: Institut für Informatik der Universität Potsdam

E-Kommunikation u. Verschlüsselung

Exkurs: Verschlüsselung 4/5

2. Gegenstand der Verschlüsselung: a) Transportverschlüsselung



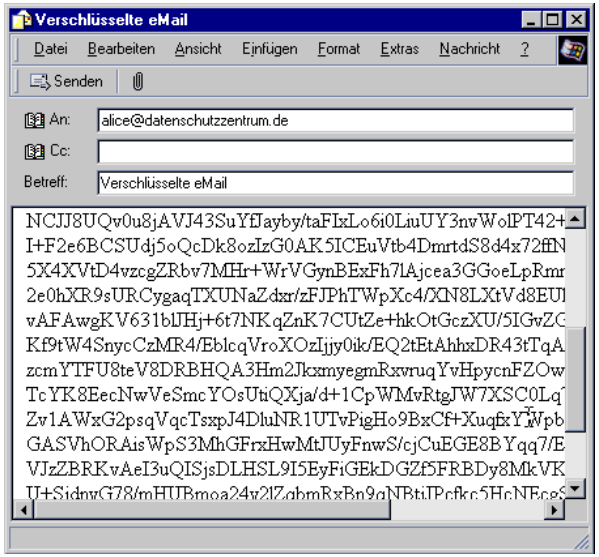
Erläuterung	Vor- und Nachteile
Aus einer offenen Rinne wird ein nicht einsehbares Rohr (z.B. https, SMTPS via SSL/TSL)	(+) Anwenderfreundlich (-) Gesamte Kette muß abgeschirmt sein (-) gehackt (Heartbleed) Beispiele: Online-Banking (https)

Quelle: http://answers.oreilly.com

E-Kommunikation u. Verschlüsselung

Exkurs: Verschlüsselung 5/5

2. Gegenstand der Verschlüsselung: b) Inhalteverschlüsselung („end to end“)



Erläuterung	Vor- und Nachteile
Unabhängig vom Transportweg wird der Inhalt der Mail verschlüsselt.	(+) Unabhängig von Sicherheit Transportweg (-) Nicht Anwenderfreundlich (Schlüsselgenerierung, -verwaltung etc.)

Quelle: https://www.datenschutzzentrum.de/selbstdatenschutz/internet/pgp/anleit2g.htm

E-Kommunikation u. Verschlüsselung

Inhalt (Forts.)

2. Verschlüsselung anbieten und *grundsätzlich* auch anwenden

- Verschlüsselung:
  - „…das Einsetzen eines Verfahrens zum Schutz der Daten vor unbefugter Einsichtnahme oder Veränderung, in dem diese mittels eines entsprechenden Algorithmus in eine nur für den Berechtigten erschließbare Form gebracht werden…“ [1]
- „grundsätzlich anzuwenden“
  - d.h. in der Regel. „…es sei denn, die jeweilige Verwaltungstätigkeit rechtfertigt davon Ausnahmen (z.B. das Versenden einer Presseinformation….“)[1].
  - Einwilligung des Betroffenen
- Art und Grad der Verschlüsselung
  - Je höher, desto höher der Grad der Vertraulichkeit der Daten[1]

[1] SMI, SächsEGovG, Handlungsleitfaden zur Umsetzung in kommunalen Behörden, Version 1.0, 6.2.2015, S. 14

E-Kommunikation u. Verschlüsselung

Inhalt (Forts.)

3. Barrierefrei

- § 7 SächsEGovG umfasst jede Form der elektronischen Kommunikation (via Internet bereits nach § 7 SächsIntegrG verpflichtend)
- Barrierefrei:
  - „ für Menschen mit Behinderungen in der allgemein üblichen Weise ohne besondere Erschwernis und grundsätzlich ohne fremde Hilfe zugänglich und nutzbar …“ (§ 3 SächsIntegrG)
- „Schrittweise“
  - Beginn der Umsetzung mit In-Kraft-Treten des SächsEGovG erforderlich.
  - Schrittweise: aufeinander folgend
  - Konzept erforderlich, in dem terminlich untersetzt ist, welche Maßnahmen wann angegangen werden

E-Kommunikation u. Verschlüsselung

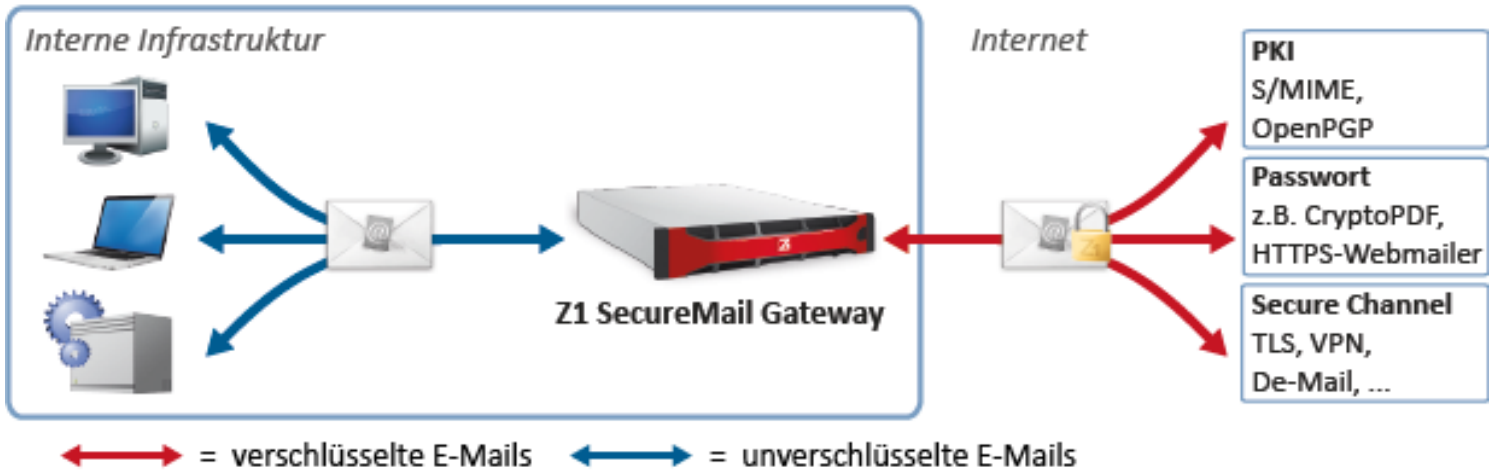
Empfehlungen zur Umsetzung

- Elektronische Kommunikation
  - „…bereits dann Rechnung getragen, wenn die elektronische Kommunikation über eine E-Mail-Adresse sichergestellt werden kann….“ [1]
- Verschlüsselung
  - Schutzbedarfsanalyse
  - End-to-End-Verschlüsselung
  - Basiskomponente „Elektronische Signatur und Verschlüsselung“ (ESV)/ Secure Mail Gateway (SMGW) Z1 (Zertificon)
  - Zertifikate
  - OSCI-Protokoll / Elektronisches Gerichts- und Verwaltungspostfach (EGVP)

[1] SMI, SächsEGovG, Handlungsleitfaden zur Umsetzung in kommunalen Behörden, Version 1.0, 6.2.2015, S. 15

E-Kommunikation u. Verschlüsselung

Empfehlungen zur Umsetzung



Quelle: https://www.zertificon.com/loesungen/email-verschluesselung-gateway

E-Kommunikation u. Verschlüsselung

Empfehlungen zur Umsetzung (Forts.)

- Barrierefreiheit
  - Orientierung an Standards für Barrierefreiheit
    - Web Content Accessibility Guidelines
    - PDF/Universal Accessibility
    - Barrierefreie-Informations-Technik Verordnung des Bundes
  - Überprüfung Ausschreibungstexte durch Träger öffentlicher Belange für Behinderte, u.a. Deutsche Zentralbücherei für Blinde
  - Überprüfung Barrierefreiheit nach Kriterien der Verordnung zur Schaffung barrierefreier Informationstechnik nach dem Behindertengleichstellungsgesetz (BITV 2.0).
  - Matterhorn-Protokoll 1.0 als Prüfkatalog für elektronische Dokumente
  - Vgl. Handlungsleitfaden, S. 51ff.

2 Übermittlung elektronischer Dokumente

Übermittlung elektronischer Dokumente

Rechtsgrundlage

Frist: 1.8.2016

§ 2 Abs. 2 SächsEGovG:

„(2) Die Übermittlung elektronischer Dokumente unter Wahrung der für den Freistaat Sachsen verbindlichen bundesrechtlichen Voraussetzungen in

1. § 3a Abs. 2 …(VwVfG),
2. § 36a Abs. 2 …(SGB I – AT)
3. § 87a Abs. 3, 4 und 6 der Abgabenordnung (AO) …,

für die **Ersetzung der Schriftform** ist durch die staatlichen Behörden und die Träger der Selbstverwaltung im Rahmen der Kommunikation nach Absatz 1 unter dem Vorbehalt der Bereitstellung von Haushaltsmitteln für die Umsetzung zu ermöglichen, soweit nicht wichtige Gründe entgegenstehen …Die …**erforderlichen Informationen** sind über die von den Behörden und Verwaltungseinrich-tungen im Freistaat Sachsen jeweils genutzten öffentlich zugänglichen Netze **zur Verfügung zu stellen.**

Frist: 1.7.2014

§ 2 Abs. 1 BEGovG:

„Jede Behörde ist verpflichtet, auch einen Zugang für die Übermittlung elektronischer Dokumente, auch soweit sie mit einer qualifizierten elektronischen Signatur versehen sind, zu eröffnen.“

Übermittlung elektronischer Dokumente

Rechtsgrundlage (Forts.)

§ 3a VwVfG - Elektronische Kommunikation

(1) Die Übermittlung elektronischer Dokumente ist zulässig, **soweit der Empfänger hierfür einen Zugang eröffnet**.

(2) Eine durch Rechtsvorschrift angeordnete Schriftform kann, soweit nicht durch Rechtsvorschrift etwas anderes bestimmt ist, durch die elektronische Form ersetzt werden. **Der elektronischen Form genügt ein elektronisches Dokument, das mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen ist.** …. Die Schriftform kann auch ersetzt werden

1. durch unmittelbare Abgabe der Erklärung in einem **elektronischen Formular**, das von der Behörde in einem Eingabegerät oder über öffentlich zugängliche Netze zur Verfügung gestellt wird;
2. bei **Anträgen und Anzeigen** durch Versendung eines elektronischen Dokuments an die Behörde mit der Versandart nach § 5 Absatz 5 des **De-Mail-Gesetzes**;
3. bei **elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörden** durch Versendung einer De-Mail-Nachricht nach § 5 Absatz 5 des **De-Mail-Gesetzes**, bei der die Bestätigung des akkreditierten Diensteanbieters die erlassende Behörde als Nutzer des De-Mail-Kontos erkennen lässt;
4. durch **sonstige sichere Verfahren**, die durch **Rechtsverordnung der Bundesregierung** mit Zustimmung des Bundesrates festgelegt werden, welche den Datenübermittler (Absender der Daten) authentifizieren und die Integrität des elektronisch übermittelten Datensatzes sowie die Barrierefreiheit gewährleisten; der IT-Planungsrat gibt Empfehlungen zu geeigneten Verfahren ab….

In den Fällen des Satzes 4 Nummer 1 muss bei einer Eingabe über öffentlich zugängliche Netze ein sicherer Identitätsnachweis nach **§ 18 des Personalausweisgesetzes** oder nach **§ 78 Absatz 5 des Aufenthaltsgesetzes erfolgen.**

Übermittlung elektronischer Dokumente

Rechtsgrundlage (Forts.)

§ 7 SächsEGovG

„Die staatlichen Behörden und die Träger der Selbstverwaltung gestalten die elektronische Kommunikation **und elektronische Dokumente schrittweise** so, dass sie auch von Menschen mit Behinderungen grundsätzlich uneingeschränkt und **barrierefrei** nach § 3 …SächsIntegrG… genutzt werden können.“

Übermittlung elektronischer Dokumente

Hintergrund

Angleichung an BEGovG, Ergänzung bundesrechtlicher Möglichkeiten

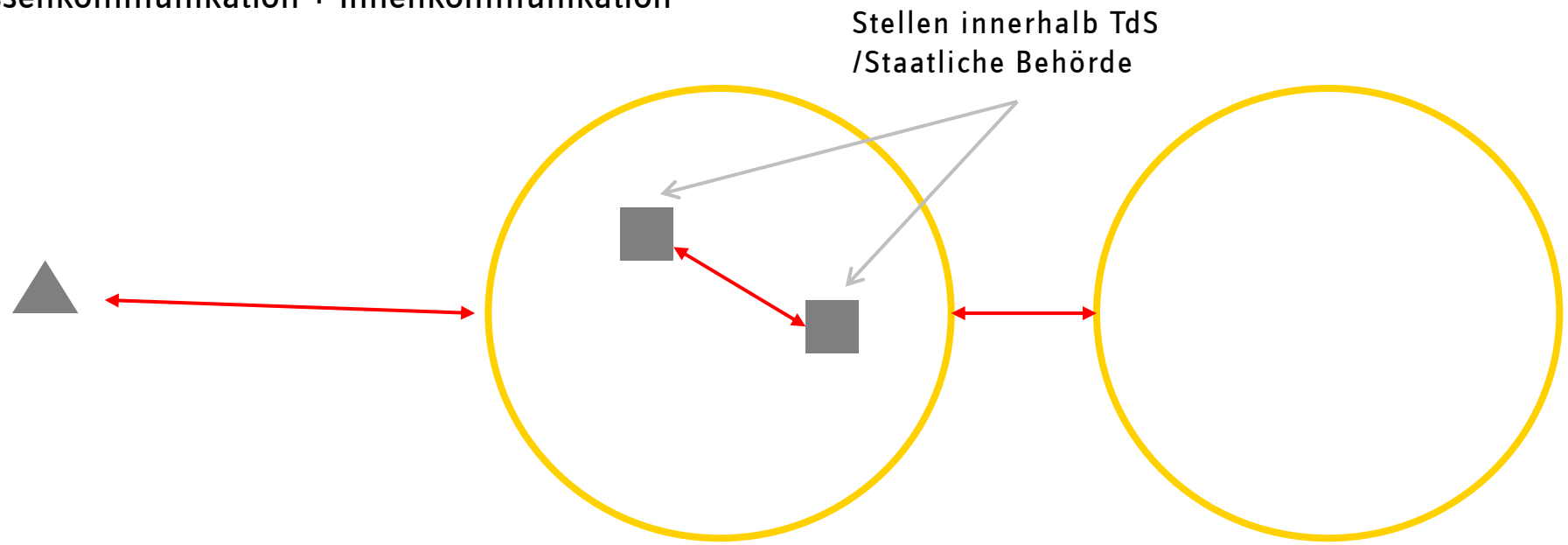
- Ca. 3.500 Schriftformerfordernisse allein im Verwaltungsrecht des Bundes (dienen u.a. **Authentizität** und **Integrität**) => Hohe Folgekosten.
- § 3a VwVfG a.F. (seit 21.8.2012)[1] nicht ausreichend: Möglichkeit des elektronischen Schriftformersatzes durch qualifizierte elektronische Signatur (qeS), aber
  - geringe Verbreitung qeS und
  - geringe (freiwillige) „Zugangseröffnung“ durch Verwaltung.
- § 3a VwVfG n.F. (Gesetz vom 25.7.2013): Erweiterung der technischen Möglichkeiten des Schriftformersatzes auf
  - elektronische Web-Formulare i.V.m. sicherer elektronischer Identifizierung (nPA oder eAT)
  - De-Mail mit Versandoption „absendebestätigt“
- Pflicht zur „Zugangseröffnung“ seit 1.7.2014, jedenfalls für Dokumente mit qeS, auch für TdS in Sachsen bei Ausführung von Bundesrecht (§ 2 Abs. 1 BEGovG)

[1] daneben in AO und SGB I und § 126a BGB

Übermittlung elektronischer Dokumente

Anwendungsbereich

Aussenkommunikation + Innenkommunikation



Übermittlung elektronischer Dokumente

Inhalt

1) Die Übermittlung elektronischer Dokumente unter Wahrung der ... Voraussetzungen ...
für die Ersetzung der Schriftform ist ... zu **ermöglichen**

- **Passiv** (Empfangen)
  - Zugangseröffnung
  - Signaturprüfung und -erhaltung (bei qeS)
- **Aktiv** (Senden)
  - Authentifizierung ermöglichen (Signaturerstellung bei qeS). Nicht bei nPA.
- **Schriftformersetzende Verfahren**
  - Dokumente mit **qualifizierter elektronische Signatur (qeS)** nach Signaturgesetz
  - **elektronische Web-Formulare** i.V.m. sicherer elektronischer Identifizierung **(nPA oder eAT mit eID-Funktion)**
  - Anträge und Anzeigen an die Behörde bzw. elektronische Verwaltungsakte oder sonstige Dokumente von der Behörde via **De-Mail mit Versandoption „absendebestätigt"**
  - **Alle 3 Verfahren -** kein Wahlrecht (praktisch aber abgemildert, s.u. Umsetzung)
  - **sonstige sichere Verfahren**, die durch Rechtsverordnung der Bundesregierung festgelegt werden - zukunftsoffen
- Veröffentlichungspflichten Behörde (§ 2 Abs. 2 S. 3 SächsEGovG)
- Frist 1.8.2016

Übermittlung elektronischer Dokumente

Qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG)

Qualifizierte elektronische Signatur

- **Sichere Signaturerstellungseinheit (SSEE)** = Software- oder Hardwareeinheiten zur Speicherung und Anwendung des jeweiligen Signaturschlüssels gem. § 17 bzw. § 23 SigG / SigVO
- **Qualifiziertes Zertifikat** = elektronische Bescheinigung, mit der Signaturprüfschlüssel einer Person zugeordnet wird und deren Identität bestätigt wird, für natürliche Personen , gültig bei Erzeugung
  - ZDA gem. §§ 4-14 SigG + Betriebsanzeige BNetzA
  - Inhalt Zertifikat gem. § 7 SigG (9 Punkte)

Beispiel:
- EGVP
- beA
- E-Mail

Jeweils mit SSEE + qualifiziertem PKI-Zertifikat

Fortgeschrittene elektronische Signatur

- die ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
- die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
- mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann,
- mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann [*Integrität*]

Beispiel:
PGP-signierte E-Mail (Prüfung Authentizität und Integrität mit Hashwert und private / public key)

Elektronische Signatur

- Daten in elektronischer Form,
- die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und
- die zur *Authentifizierung* dienen

Beispiel:
Normale E-Mail („mit freundlichen Grüßen gez. Meier")

Übermittlung elektronischer Dokumente

Qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG) – Forts.

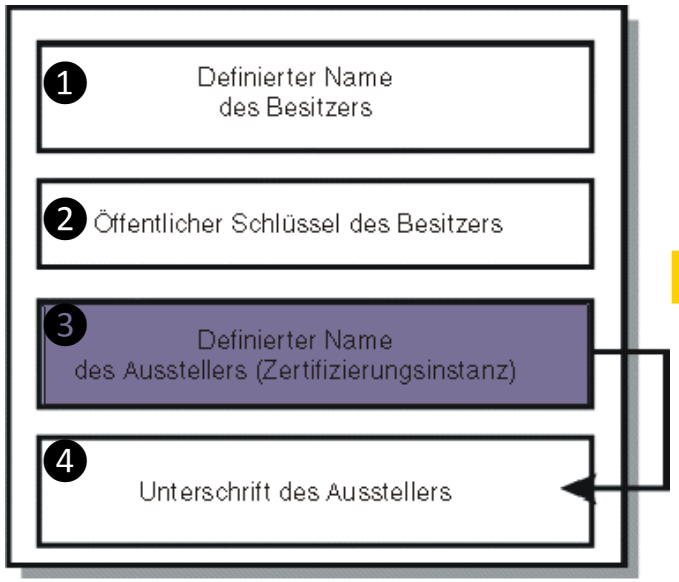
Sichere Signaturerstellungseinheit

Quelle: https://www.chipkartenleser-shop.de/shop/rsct/article/4544

Übermittlung elektronischer Dokumente

Qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG) – Forts.

X-509-v3-Zertifikat



Quelle: Wikipedia; http://publib.boulder.ibm.com/tividd/td/TRM/SC23-4822-00/de_DE/HTML/user276.htm

Beispiel (Textdarstellung nach Lesbarmachung mit Interpreter)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1 (0x1)
        Signature Algorithm: md5WithRSAEncryption
3       Issuer: C=AT, ST=Steiermark, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/Email=ca@trustme.dom
        Validity
            Not Before: Oct 29 17:39:10 2000 GMT
            Not After : Oct 29 17:39:10 2001 GMT
1       Subject: C=AT, ST=Vienna, L=Vienna, O=Home, OU=Web Lab, CN=anywhere.com/Email=xyz@anywhere.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
2               Modulus (1024 bit):
                    00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
                    d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
                    9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
                    90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
                    1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
                    7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
                    50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
                    8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
                    f0:b4:95:f5:f9:34:9f:f8:43
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                email:xyz@anywhere.com
            Netscape Comment:
                mod_ssl generated test server certificate
4           Netscape Cert Type:
                SSL Server
    Signature Algorithm: md5WithRSAEncryption
        12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
        3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
        82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
        cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
        4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
        d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
        44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
        ff:8e:
```

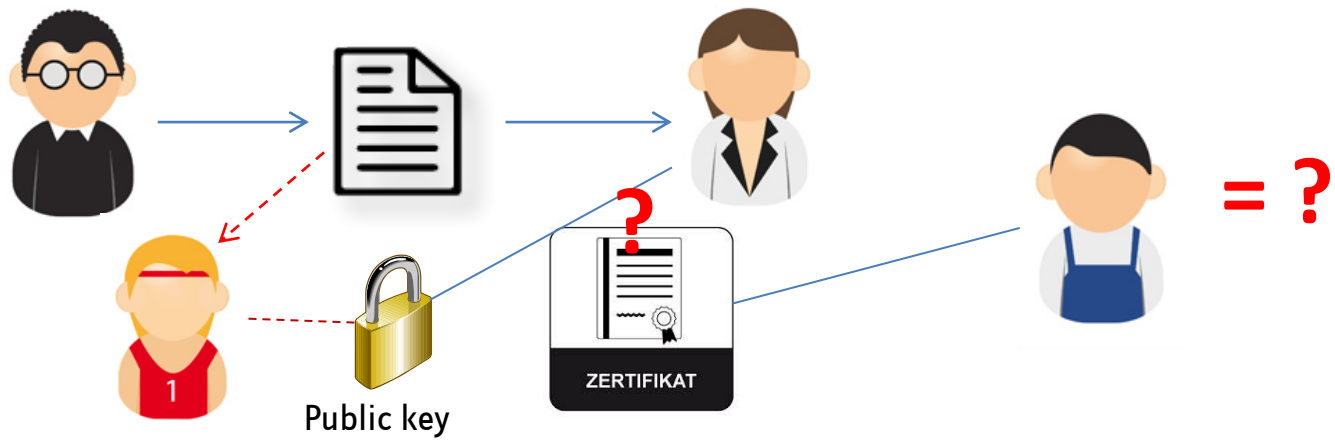
Übermittlung elektronischer Dokumente

Qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG) – Forts.

Funktion Zertifikat

- Problem Zuordnung Public Key
- Lösung: Bestätigung eines (vertrauenswürdigen) Dritten

  Zertifikat = Signatur des öffentlichen Schlüssels = Hashwert des öffentlichen Schlüssels wird mit privatem Schlüssel des Ausstellers verschlüsselt



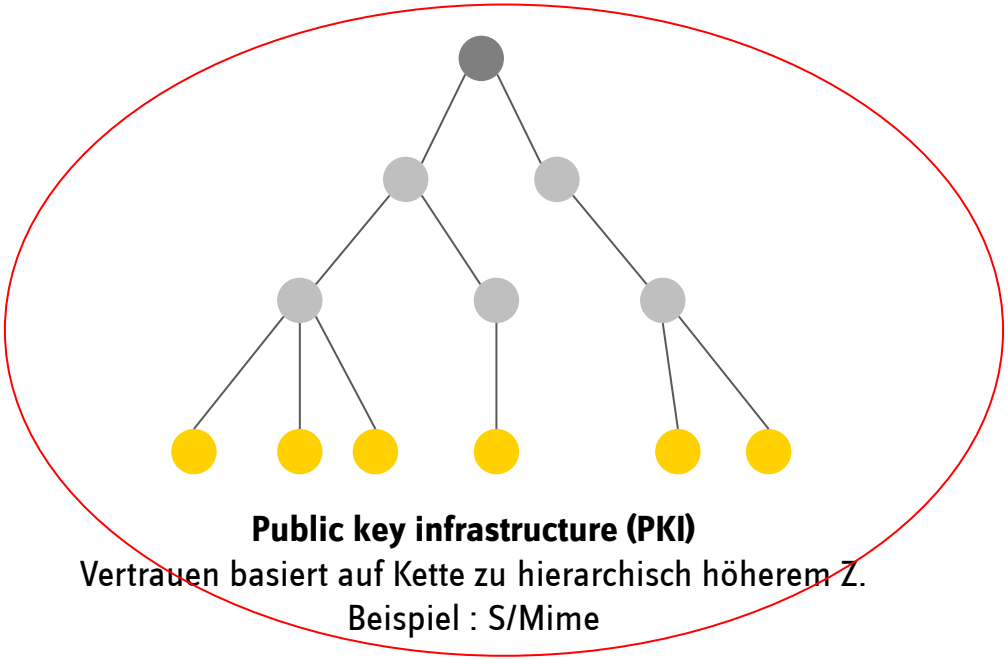
Quelle: http://billatnapier.wordpress.com/2013/05/04/the-nightmare-that-is-pki-and-digital-certificates/
http://www.grafiker.de/kreativ-news/02092009/people-icon-set-klappe-die-dritte

Übermittlung elektronischer Dokumente

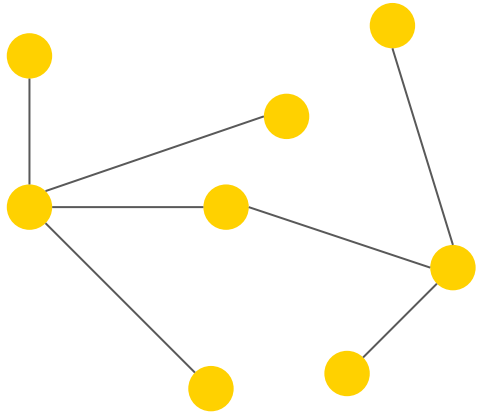
Qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG) – Forts.

Problem Vertrauen in Aussteller Zertifikat und Zuordnung Zertifikat / Aussteller

- 2 Lösungsansätze:



Public key infrastructure (PKI)
Vertrauen basiert auf Kette zu hierarchisch höherem Z.
Beispiel : S/Mime



Web of Trust
Vertrauen basiert auf Zahl der P2P Zertifikate
Beispiel: OpenPGP

Quelle: https://de.wikipedia.org/wiki/Web_of_Trust; http://www.cio.bund.de/Web/DE/IT-Angebot/IT-Beratungsdienstleistungen/Public-Key-Infrastruktur-der-Verwaltung/public_key_node.html

Übermittlung elektronischer Dokumente

Qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG) – Forts.

Anwendungen mit qualifizierter elektronischer Signatur

- E-Mail / SMTP-Protokoll
- EGVP / OSCI-Protokoll[1]
- besonderes elektronisches Anwalts (Notar) -Postfach (beA/beN) / OSCI-Protokoll[2]
- nPA mit Unterschriftsfunktion (≠ eID-Funktion)

Signaturdatei (z.B. *.pkcs7) und Nutzdatei

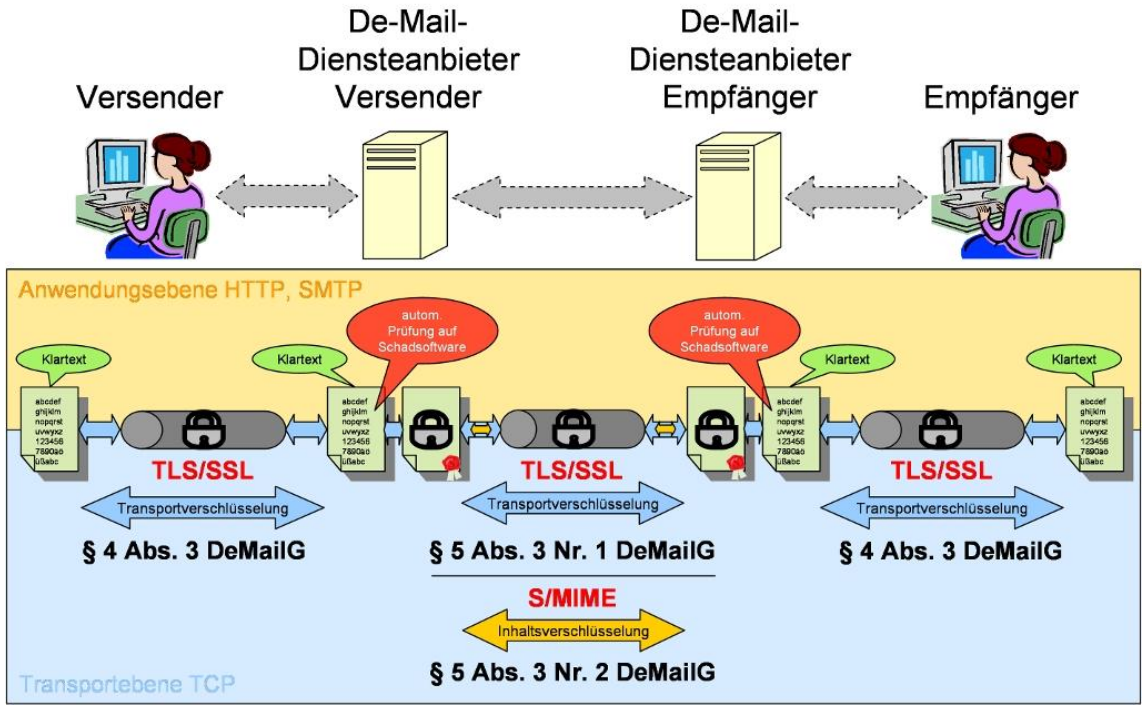
- in getrennten Dateien (von Gerichten gewünscht)
- in Containerdatei, die Nutzdatei und Signatur enthält
- Signatur in Nutzdatei enthalten („inline"), so z. B. bei PDF oder XML

[1] auch lediglich fortgeschrittene Signatur möglich

[2] ab 2018 bei Versand durch Rechtsanwälte nicht mehr erforderlich; beA gilt dann als sicherer Übertragungsweg, wie De-Mail

Übermittlung elektronischer Dokumente

De-Mail



Erläuterung	Vor- und Nachteile	Beispiele
Proprietäres System (von De-Mail zu De-Mail). Zusätzlicher Kanal zu Brief und E-Mail. Schwerpunkt Authentifizierung (ersetzt nicht Briefumschlag, sondern Einschreiben). Standardmäßig nur Transportverschlüsselung	(-) Kein offenes System (-) End-to-End-Verschlüsselung nur als Option möglich, umständlich, fraglich (CCC 2011)	Verschiedene akkreditierte Anbieter (u.a. DeTAG, 1&1 mit GMX, Web.de)

Übermittlung elektronischer Dokumente

Neuer Personalausweis (nPA)

3 Funktionen

- eID-Funktion (sicherer Internet-Ausweis) – schriftformersetzend bei „unmittelbarer Abgabe der Erklärung in einem elektronischen Formular, das von der Behörde … über öffentlich zugängliche Netze zur Verfügung gestellt wird“ (§ 3a Abs. 2 Satz 4 Nr. 1, Satz 5 VwVfG)
- Unterschriftsfunktion (nPA als Signaturkarte) – schriftformersetzend in Verbindung mit qeS (nach § 3a Abs. 2 Satz 4 Nr. 3 VwVfG)
- Reisedokument - Ausweisfunktion

Quelle: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeAusweise/Personalausweis/personalausweis_node.html

Übermittlung elektronischer Dokumente

Inhalt (Forts.)

2) Vorbehalte

- Vorbehalt der Bereitstellung von Haushaltsmitteln
  - Umsetzung erfordert erhebliche finanzielle und organisatorische Aufwendungen

- Wichtige Gründe:
  - FS plant zentrale Unterstützung über Basiskomponenten und gemeinsame Berechtigungszertifikate auch für TdS. Solange und soweit dies noch der Fall ist, liegt ein wichtiger Grund vor, ggf. auch für Zugang für Dokumente mit qeS **(Gesetzesbegründung zu § 2 Abs. 2)**
  - vgl. aktuellen Stand

- Trotz Vorbehalte: **Ein** Zugangsweg (z.B. qeS, weil nach BEGovG ohnehin Pflicht) wird jedenfalls eröffnet werden müssen
  - vgl. Handlungsleitfaden, S. 29; Gesetzesbegründung, S. 38

Übermittlung elektronischer Dokumente

Empfehlungen zur Umsetzung

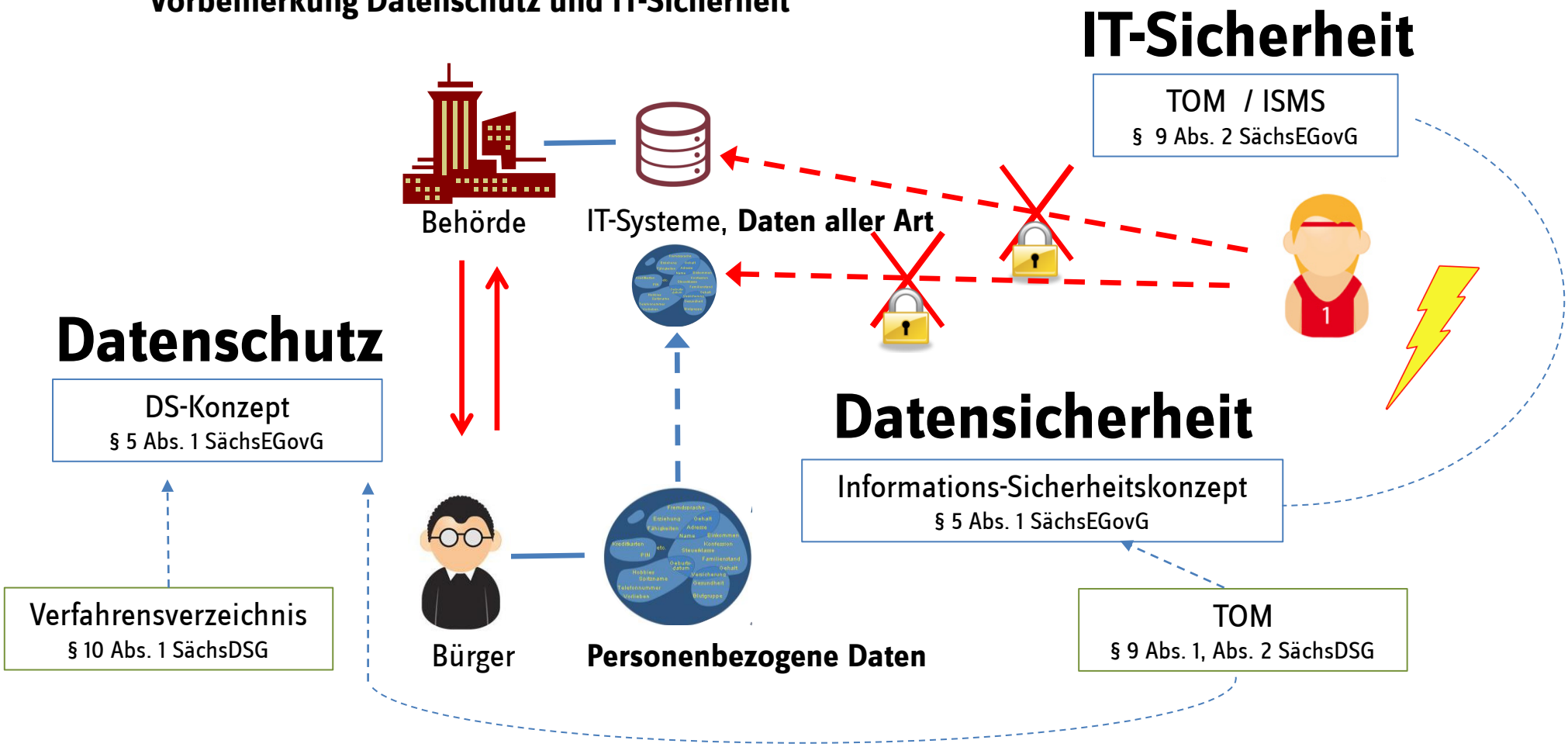
Empfehlung: Mitnutzung gemeinsamer Basiskomponenten des FS (BaK „ESV“)

- Generelle Anforderung: Signatur-Workflow sicherstellen:
  - Signaturerstellung (Unterschreiben), -prüfung (Kontrolle / Akzeptanz), -erhaltung (beweiswerthaltige Speicherung)
- Erweiterung BaK ESV zur Zeit in Testphase mit verschiedenen Varianten.
  - Wird zum 1.8.2016 verfügbar sein (VO auf Basis von § 10 Abs. 4 SächsEGovG, verpflichtende Nutzung durch staatliche Behörden).
  - Nutzung durch TdS im Rahmen der Nutzungsvereinbarung vom 20.8.2014; Mitfinanzierung im Rahmen von § 29a Abs. 2 Sächsisches FAG (s.u. Abschnitt Basiskomponenten)

3 Datenschutz

Datenschutz

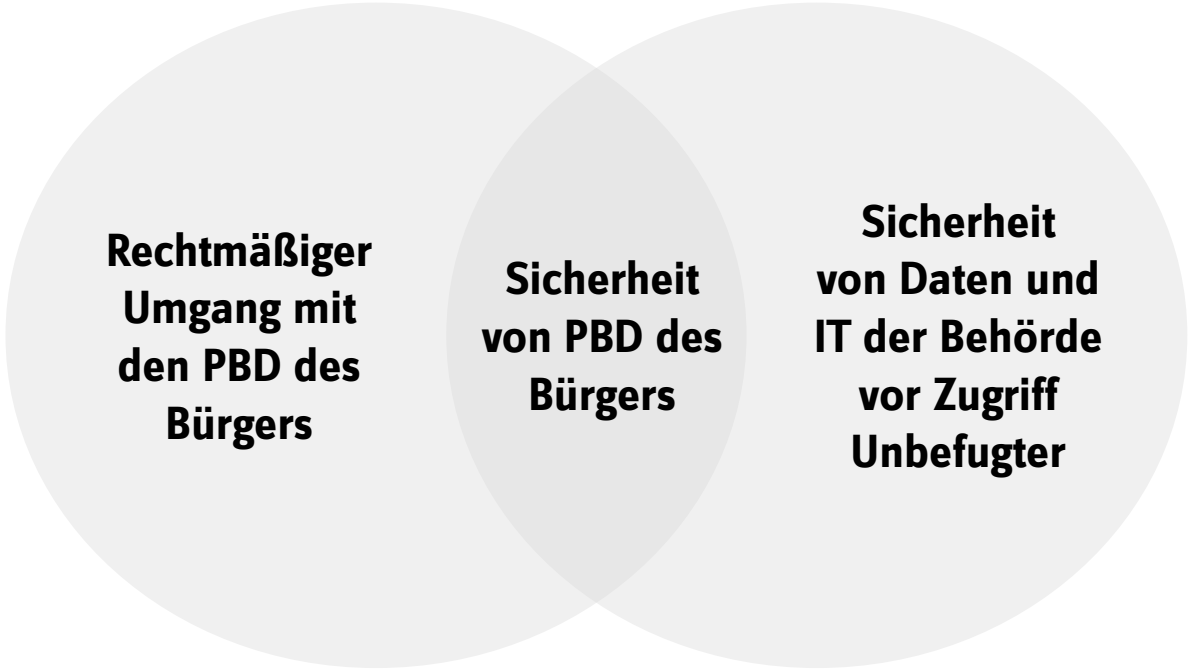
Vorbemerkung Datenschutz und IT-Sicherheit



Quelle: http://www.grafiker.de/kreativ-news/02092009/people-icon-set-klappe-die-dritte; https://www3.sachsen.schule/thema-datenschutz/start/

Datenschutz

Vorbemerkung Datenschutz und IT-Sicherheit (Forts.)



Datenschutz

Vorbemerkung Datenschutz und IT-Sicherheit (Forts.)

	Datenschutz	IT-Sicherheit
Schutzobjekt	Person	Organisation
Angreifer	Organisation	Person, Technik, Natur
„Gewährleistungs“[5]-/ Schutzziele	• Verfügbarkeit [1, 5] • Vertraulichkeit [1, 4, 5] • Integrität [1, 4, 5] • Authentizität [1] • Revisionsfähigkeit [1] • Transparenz [1, 4] • Intervenierbarkeit [2, 5] • Nicht-Verkettbarkeit [3, 5] • Datensparsamkeit [5, 6]	• Verfügbarkeit [1] • Vertraulichkeit [1, 4] • Integrität [1, 4] • Authentizität [1] • Revisionsfähigkeit [1] • Transparenz [1, 4]
Anwendungsbereich	Personenbezogene Daten	Daten aller Art

[1] vgl. § 9 Abs. 2 SächsDSG bzw. § 9 Abs. 2 SächsEGovG
[2] vgl. § 5 Abs. 1 Nr. 6 LDSG SH, §§ 18-23 SächsDSG
[3] vgl. § 5 Abs. 1 Nr. 5 LDSG SH, § 13 SächsDSG
[4] vgl. Art. 5 DSGVO
[5] vgl. DSBK 2015: SDM-Handbuch, V0.9a
[6] vgl. § 9 Abs. 1 Satz 2 SächsDSG

Datenschutz

Vorbemerkung Datenschutz und IT-Sicherheit (Forts.)

Schutzziele nach § 9 Abs. 2 SächsDSG und § 9 Abs. 2 SächsEGovG

Vertraulichkeit	nur Befugte können pbD / D zur Kenntnis nehmen
Integrität	pbD / D bleiben während der Verarbeitung unversehrt, vollständig und aktuell
Verfügbarkeit	pbD / D stehen zeitgerecht zur Verfügung und können ordnungsgemäß verarbeitet werden
Authentizität	pbD / D können jederzeit ihrem Ursprung zugeordnet werden
Revisionsfähigkeit	Es kann festgestellt werden, wer wann welche pbD / D in welcher Weise verarbeitet hat
Transparenz	die Verfahrensweisen bei der Verarbeitung pbD / D sind vollständig, aktuell und in einer Weise dokumentiert, dass sie in zumutbarer Zeit nachvollzogen werden können

Datenschutz

Rechtsgrundlage

Frist: 9.8.2014

§ 5 Abs. 1 SächsEGovG:

Zur Gewährleistung des Datenschutzes erstellen und pflegen die staatlichen Behörden und die Träger der Selbstverwaltung, die **personenbezogene Daten automatisiert verarbeiten, Datenschutz-** und Informationssicherheits**konzepte**.

Datenschutz

Rechtsgrundlage (Forts.)

§ 9 SächsDSG Abs. 1 und 2

(1) Öffentliche Stellen, die personenbezogene Daten verarbeiten, haben **alle angemessenen personellen, technischen und organisatorischen Maßnahmen** zu treffen, die erforderlich sind, um eine den Vorschriften dieses Gesetzes entsprechende Datenverarbeitung zu gewährleisten. Die Grundsätze der **Datenvermeidung und Datensparsamkeit** sind zu beachten.

(2) Werden personenbezogene Daten verarbeitet, sind nach dem jeweiligen Stand der Technik Maßnahmen zu treffen, die geeignet sind zu gewährleisten, dass

1. nur Befugte personenbezogene Daten zur Kenntnis nehmen können **(Vertraulichkeit),**
2. personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben **(Integrität),**
3. personenbezogene Daten zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können **(Verfügbarkeit),**
4. jederzeit personenbezogene Daten ihrem Ursprung zugeordnet werden können **(Authentizität),**
5. festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat **(Revisionsfähigkeit),**
6. die Verfahrensweisen bei der Verarbeitung personenbezogener Daten vollständig, aktuell und in einer Weise dokumentiert sind, dass sie in zumutbarer Zeit nachvollzogen werden können **(Transparenz).**

Datenschutz

Rechtsgrundlage (Forts.)

§ 10 SächsDSG

(1) Jede datenverarbeitende Stelle führt **ein Verzeichnis der bei ihr eingesetzten automatisierten Verarbeitungsverfahren.** In dem Verzeichnis sind schriftlich festzulegen: …8. **die personellen, technischen und organisatorischen Maßnahmen gemäß § 9,**

(3) Die datenverarbeitenden Stellen sind verpflichtet, **dem Sächsischen Datenschutzbeauftragten** vor dem erstmaligen Einsatz eines automatisierten Verarbeitungsverfahrens das Verzeichnis im Sinne des Absatzes 1 **zuzuleiten**. Die datenverarbeitende Stelle bringt das von ihr geführte Verzeichnis **regelmäßig auf den neuesten Stand** …

(4) Vor dem erstmaligen Einsatz oder der wesentlichen Änderung
1. eines Verfahrens nach § 8,
2. eines automatisierten Verfahrens, in dem Daten im Sinne des § 4 Abs. 2 verarbeitet werden oder
3. eines automatisierten Verfahrens, in dem Daten von Beschäftigten im Sinne des § 37 verarbeitet werden,

ist durch den Sächsischen Datenschutzbeauftragten …zu prüfen, ob die Datenverarbeitung zulässig ist und die vorgesehenen Maßnahmen nach § 9 ausreichend sind **(Vorabkontrolle)**. Die datenverarbeitende Stelle hat ihm dazu die erforderlichen Unterlagen zur Verfügung zu stellen….

Datenschutz

Hintergrund

Konkretisierung von Pflichten nach SächsDSG für E-Government

- Schutzziel: Schutz der Bürger / Mitarbeiter und ihrer personenbezogenen Daten
- Konkretisierung von § 9 SächsDSG (Pflicht zur Erstellung von Datenschutz- und Informationssicherheitskonzepten) und von § 10 Abs. 1 Satz 2 Nr. 8 SächsDSG (Aufnahme in die schriftlichen Verzeichnisse)
- Voraussetzung: Automatisierte Verarbeitung (vgl. Definition in § 3 Abs. 5 SächsDSG) von Personenbezogenen Daten → **Fokus auf Schutz der Personenbezogenen Daten**
- Personenbezogenen Daten im E-Government
  - von Bürgern
  - von Mitarbeitern der Behörden

Datenschutz

Inhalt

1. Datenschutzkonzept erstellen und pflegen

- Datenschutzkonzept:

  Dokument, das Auskunft über die Rechtmäßigkeit der Datenverarbeitung bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten gibt.

  > „Das Datenschutzkonzept dokumentiert für die datenschutzrechtliche Beurteilung notwendige Informationen zur Verarbeitung personenbezogener Daten, auch im Hinblick auf Art, Umfang, Tiefe und Ausmaß der Verarbeitung personenbezogener Daten.“ [1]

- Funktion: Eigenkontrolle (Datenschutz = Daueraufgabe) und Revisionsunterlage
- Ziele: Datenschutz
- Schutzobjekt / Angreifer: Person → Behörde

[1] SMI, SächsEGovG, Handlungsleitfaden zur Umsetzung in kommunalen Behörden, Version 1.0, 6.2.2015, S. 38

Verfahrensverzeichnis gemäß § 10 SächsDSG
Verfahren (Bezeichnung):
Aktenzeichen:
neues Verfahren / Änderung
Das Verfahren ist zur Einsichtnahme bestimmt ja/nein

Beispiel
(nach https://www.datenschutzzentrum.de/ verfahrensverzeichnis)

1. Name und Anschrift der Daten verarbeitenden Stelle
   1.1 Name und Anschrift
   1.2 Organisationskennziffer, Amt, Abteilung, ggf. Sachgebiet
   1.3 Kontaktdaten für Betroffene
2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung
   2.1 Zweckbestimmung
   2.2 Rechtsgrundlage (ggf. nach Art der Datenverarbeitung unterscheiden)
3. Kreis der Betroffenen (lfd. Nr.)
4. Kategorien der verarbeiteten Daten und Löschungs- bzw. Aufbewahrungsfristen
   4.1 Kategorien der verarbeiteten Daten (lfd. Nr. / Datum nach § 4 Abs. 2 SächsDSG (ja/nein))
   4.2 Löschungs- und Aufbewahrungsfristen (Daten aus Nr. 4.1 / Datum)
   4.3. Zugriffsberechtigte Personen oder Personengruppen (Daten aus Nr. 4.1 / Person)
5. Art und Empfänger zu übermittelnder Daten sowie Art und Herkunft empfangener Daten (inkl. Auftragsdatenverarbeitung)
   5.1 Empfänger von zu übermittelnden Daten (Daten aus Nr. 4.1 / Empfänger)
   5.2 Herkunft empfangener Daten (Daten aus Nr. 4.1 / Sender)
6 Übermittlung an Stellen außerhalb der Mitgliedstaaten der Europäischen Union nein / ja (aufgeführt in Punkt 5.2)
7. Allgemeine Beschreibung der nach § 9 SächsDSG zur Einhaltung der Datensicherheit getroffenen Maßnahmen
8. Datenschutzrechtliche Beurteilung
   8.1 Rechtsgrundlagen und Zweckbestimmung
   8.2 Technisch-organisatorische Maßnahmen
   - Verfügbarkeit (personenbezogene Daten stehen zeitgerecht zur Verfügung und können ordnungsgemäß verarbeitet werden):
   - Vertraulichkeit (es können nur Befugte personenbezogene Daten zur Kenntnis nehmen):
   - Integrität (es wird gewährleistet, dass personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell bleiben):
   - Authentizität (personenbezogene Daten können jederzeit ihrem Ursprung zugeordnet werden):
   - Transparenz (die Verfahrensweisen bei der Verarbeitung personenbezogener Daten sind vollständig, aktuell und in einer Weise dokumentiert, dass sie in zumutbarer Zeit nachvollzogen werden können):
   - Intervenierbarkeit (die Daten verarbeitende Stelle kann nachweisen, dass sie den Betrieb ihrer informationstechnischen Systeme steuernd beherrscht und dass Betroffene die ihnen zustehen Rechte ausüben können):
   - Revisionsfähigkeit (es kann festgestellt werden, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat
   - Nicht-Verkettbarkeit (es kann sichergestellt werden, dass Daten nur zu dem ausgewiesenen Zweck automatisiert erhoben, verarbeitet und genutzt werden):
   - Datensparsamkeit und -vermeidung (es werden so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt):
9. Freigabe des Verfahrensverzeichnisses

Datenschutz

Inhalt

2. Informationssicherheitskonzept erstellen und pflegen

- Informationssicherheitskonzept Datenschutz
  - Beschreibung technischer, personeller und organisatorischer Maßnahmen, mit denen **Personenbezogene Daten** gegen verschiedenen Risiken geschützt werden können
  - Sinnvoll: Einbeziehung des Schutzes von **Nicht Personenbezogenen Daten und IT** [1].
- Funktion: Eigenkontrolle (Datenschutz = Daueraufgabe) und Revisionsunterlage
- Ziele: Schutzziele gem. § 9 Abs. 2 SächsDSG (vor allem IT-Sicherheit)
- Schutzobjekt / Angreifer: vor allem Behörde -> Dritte
- Maß für Angemessenheit Vorkehrung: Verhältnis Aufwand und Folge Schutzzielverletzung (vgl. auch § 9 Satz 2 BDSG)

[1] vgl. Punkt „Informationssicherheit“ und „Musterleitlinie Informationssicherheit für die Träger der kommunalen Selbstverwaltung“ der SAKD

Datenschutz

Empfehlungen zur Umsetzung

- Vorbereitung
  - Verantwortlichkeiten im Datenschutz festlegen (Führungskräfte und DSB, § 11 SächsDSG)
  - Verpflichtung der Mitarbeiter auf das Datengeheimnis (§ 6 Abs. 2 SächsDSG)
  - Verfahrensverzeichnis führen (§ 10 Abs. 1 S. 1 SächsDSG)
  - Ggf. Vorabkontrolle (§ 10 Abs. 4 SächsDSG) durch DSB - Anzeigepflicht
- Konzepte erstellen
  - Festlegung Daten und Zweck der Datenverarbeitung und des rechtlichen Rahmens
  - Prüfung der Grundsätze der Geeignetheit, Erforderlichkeit, Zweckbindung der Datenverwendung, Datenvermeidung, Datensparsamkeit
  - Ermittlung Schutzbedarf der Daten (z.B. Normal, Hoch, Sehr hoch nach BSI)
  - Aufzählung und Beschreibung der eingesetzten IT-Komponenten
  - Prozessbezogene Verfahrensbeschreibung
  - Dokumentation der techn. / organ. Maßnahmen (z.B. BSI-GS) je Schutzziel
  - Weitere Festlegungen (Rollen und Zugriffsrechte, Löschung von Daten, Protokollierung, Auftragsdatenverarbeitung nach § 7 SächsDSG)

Datenschutz

Leitfäden und Empfehlungen

- Handlungsleitfaden, S. 39-49, Checkliste zur Erstellung von Datenschutz- und Informationssicherheitskonzepten, Stand Dezember 2014, in: Anlage zum Handlungsleitfaden (6 Seiten)
- Standard-Datenschutzmodell v 0.9, Stand 1.10.2015 (Konferenz der Datenschutzbeauftragten des Bundes und der Länder)
- Bekanntmachung des SächsDSB zur Bestellung von DSB öffentlicher Stellen vom 11.3.2004
- Musterdienstanweisung über die Organisation des Informations- und Datenschutzes
- BSI-Maßnahmenkataloge M 2.502 , M 2.503 Datenschutz
- Merkblatt des SächsDSB zur Verpflichtung auf das Datengeheimnis
- Formblätter für die Verpflichtung
- Bekanntmachung des SächsDSB zur Vorabkontrolle
- Hinweise zur Schutzbedarfsfeststellung im BSI-Standard 100-2
- Baustein B 1.5 Datenschutz – BSI
- Rollenkonzept zur E-Government Plattform des FS Sachsen
- Orientierungshilfe „Sicheres Löschen magnetischer Datenträger“
- Orientierungshilfe „Protokollierung“, AK „Technische und organisatorische DS-Fragen
- Mustervertrag Auftragsdatenverarbeitung gem. § 7 SächsDSG

4 IT-Sicherheit

Informationssicherheit

Rechtsgrundlage

Frist: 9.8.2014

„Die staatlichen Behörden treffen **angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen** zur Einhaltung der in § 9 Abs. 2 SächsDSG definierten Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Revisionsfähigkeit und Transparenz **für die in ihren informationstechnischen Systemen verarbeiteten Daten.** Solche Maßnahmen sind **angemessen**, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen einer Verletzung der Schutzziele steht.“**(§ 9 Abs. 2 S. 1, 2 SächsEGovG)**

„Für die an E-Government beteiligten Träger der Selbstverwaltung gilt § 9 Abs. 2 Satz 1 und 2 entsprechend.“
(§ 13 Abs 1 SächsEGovG)

„Der IT-Kooperationsrat beschließt, soweit kommunale Belange berührt werden, Empfehlungen für die Kommunen und die staatlichen Behörden insbesondere zu … 5. landesspezifischen Interoperabilitäts-und **Informationssicherheitsstandards für verwaltungsebenenübergreifende elektronische Verwaltungsprozesse** der im Freistaat Sachsen eingesetzten informationstechnischen Systeme…“ **(§ 18 Abs. 3)**

Informationssicherheit

Rechtsgrundlage SVN-Anbindung

Frist: 9.8.2014

„Die **verwaltungsebenenübergreifende** elektronische Datenübermittlung im Sinne von § 11 zwischen den staatlichen Behörden und den Trägern der Selbstverwaltung wird über das **Sächsische Verwaltungsnetz** geführt. Die kommunalen Träger der Selbstverwaltung können dabei den Zugang zu dem Sächsischen Verwaltungsnetz über das Kommunale Datennetz und die nichtkommunalen Träger der Selbstverwaltung über einen unmittelbaren Anschluss herstellen. Alternativ können die Träger der Selbstverwaltung den Zugang zu dem Sächsischen Verwaltungsnetz über eine Schnittstelle herstellen, die eine vergleichbare Funktionalität und eine gleichwertige Informationssicherheit gewährleistet. Satz 1 gilt nicht, soweit für einzelne Fachverfahren spezielle Rechtsvorschriften eine zuverlässige und sichere Datenübermittlung gewährleisten. „**(§ 15 Abs. 1 SächsEGovG)**

„Die Staatsregierung wird ermächtigt, die Eigenschaften der Schnittstelle gemäß Absatz 1 Satz 3 durch **Rechtsverordnung** näher zu bestimmen, soweit dies zur Wahrung der Voraussetzungen des Absatzes 1 Satz 3 erforderlich ist.“ **(§ 15 Abs. 2 S. 1 SächsEGovG)**

„Der IT-Kooperationsrat beschließt, soweit kommunale Belange berührt werden, **Empfehlungen** für die Kommunen und die staatlichen Behörden insbesondere zu … 6. …den Anforderungen an die alternative Schnittstelle für den Netzzugang gemäß § 15 Abs. 1 Satz 3 und Abs. 2 … **(§ 18 Abs. 3 SächsEGovG)**

Informationssicherheit

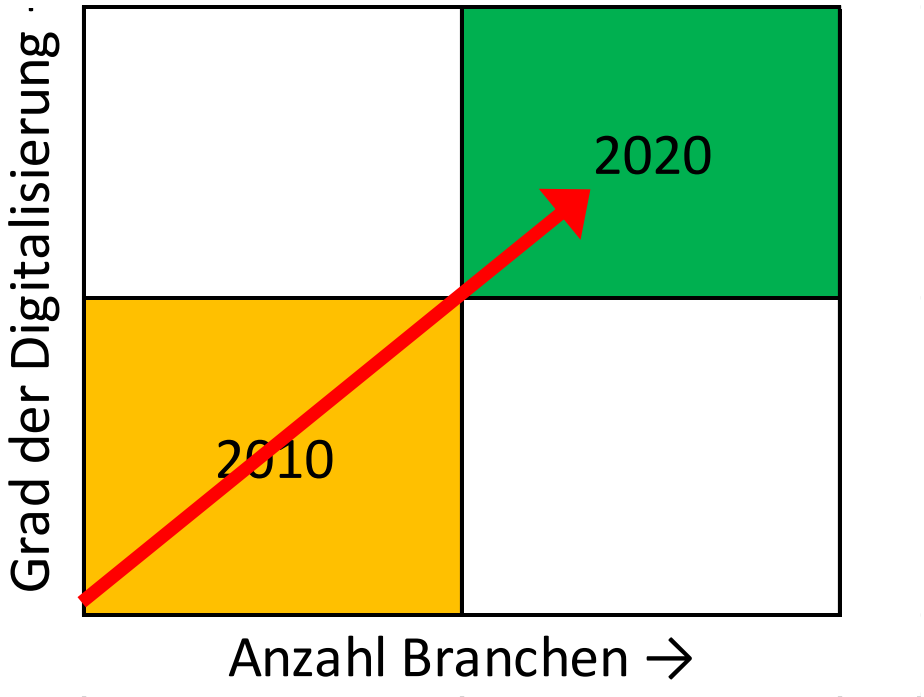
Hintergrund

- Adaption der Schutzziele nach § 9 SächsDSG auf die IT-Sicherheit
- Schutzziel: IT-Sicherheit, nicht Datenschutz, d.h.
  - Schutz der Behörde
  - alle Daten und Systeme.
- Ergänzung des IT-Sicherheitsgesetzes (staatliche Behörden sind nicht vom ITSG erfasst !).

Informationssicherheit

Hintergrund (Forts.)

Zunehmende digitale Transformation aller gesellschaftlichen Bereiche

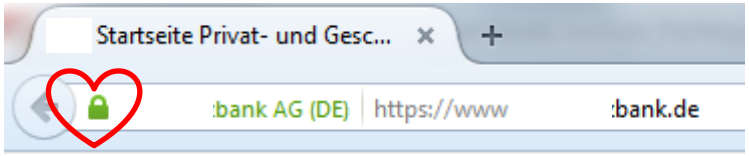


* Quelle: http://www.bain.com/publications/articles/leading-a-digical-transformation.aspx; www.pwc.ch/digital

Informationssicherheit

Hintergrund (Forts.)

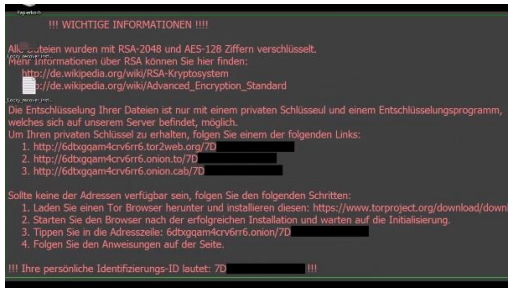
IT-Sicherheitslage angespannt, zunehmend Angriffe auf KRITIS inkl. Staat

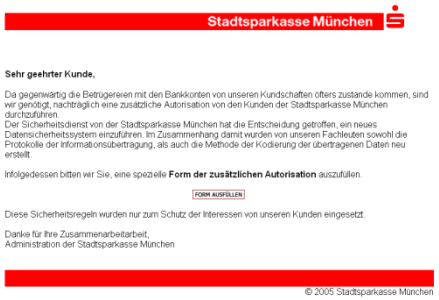


Bedrohungen	2013	2014	Prognose
Schwachstellen	↑	→	→
Spam	↓	↑	→
Schadprogramme	↑	↑	↑
Drive-by-Exploits und Exploit-Kits	↑	→	→
Botnetze	→	→	→
Social Engineering	→	↑	→
Identitätsdiebstahl	↑	↑	↑
Denial of Service (DoS; DDoS)	→	→	→
Advanced Persistent Threats (APT)	↑	→	↑

↑ Steigend → Gleichbleibend ↓ Sinkend

Stuxxnet 2010; Duqu 2011; Flame 2012; Gauss 2012; Roter Oktober 2013; NetTraveler 2013; Icefog 2013; Regin 2014; Angriff auf D. Bundestag 2015





Quelle: BSI: Die Lage der IT-Sicherheit in Deutschland 2014; http://www.secupedia.info/wiki/Advanced_Persistent_Threat; http://www.secureworks.com/cyber-threat-intelligence/advanced-persistent-threats/understand-threat/ which must be credited when shared based on creative commons terms of use defined here http://www.secureworks.com/contact/terms_of_use/; Wikipedia, SW "Phishing"; http://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html

Informationssicherheit

Inhalt

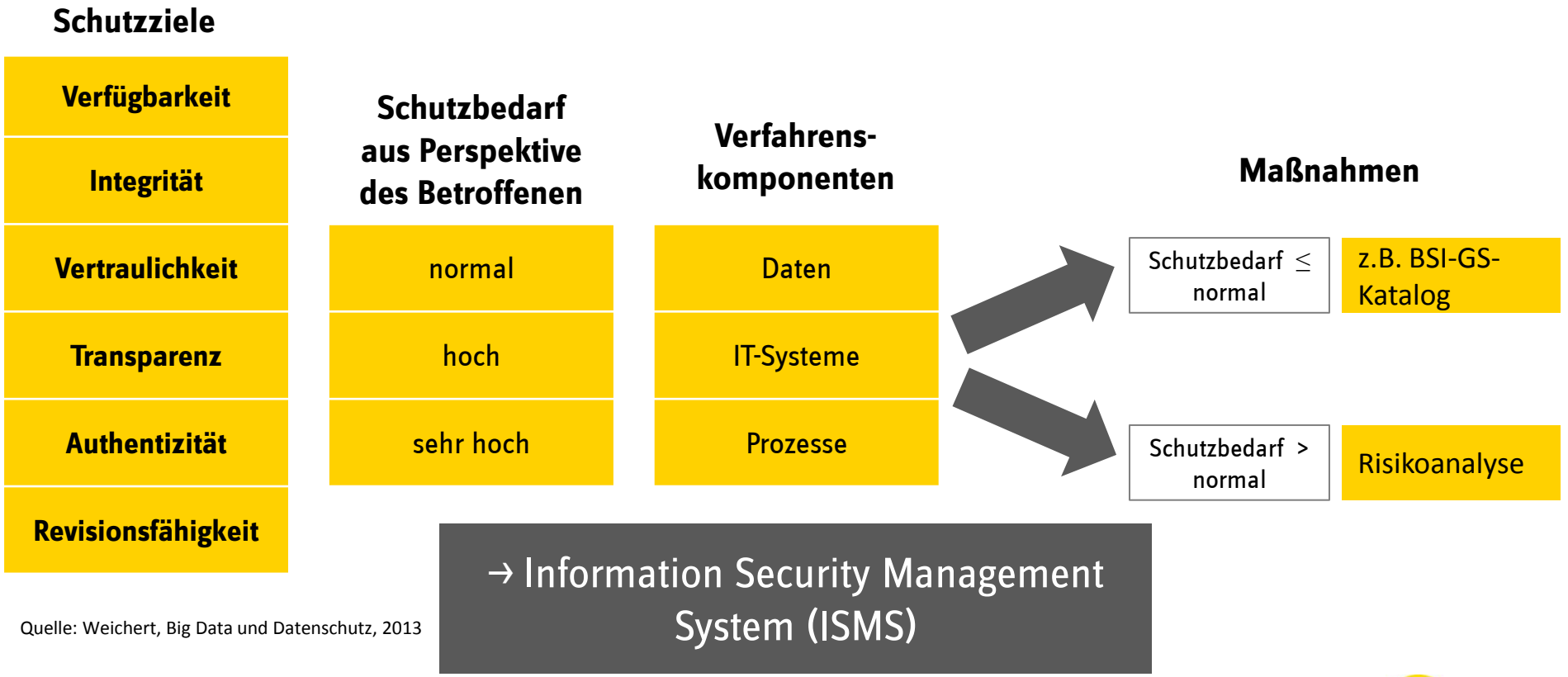
Technische-Organisatorische Maßnahmen zur Gewährleistung der Info.-Sicherheit

- Schutzziele: § 9 Abs. 2 SächsEGovG i.V.m. § 9 Abs. 2 SächsDSG, vor allem
  - Verfügbarkeit
  - Integrität
  - Vertraulichkeit
  - Authentizität
- Schutzgegenstand: IT, Daten aller Art
- Schutzobjekt / Angreifer: Behörde -> Dritte
- Maß für Angemessenheit Vorkehrung: Verhältnis Aufwand und Folge Schutzzielverletzung (§ 9 Abs. 2 Satz 2 SächsEGovG)

Informationssicherheit

Inhalt (Forts.)

Technische-Organisatorische Maßnahmen zur Gewährleistung der Info.-Sicherheit



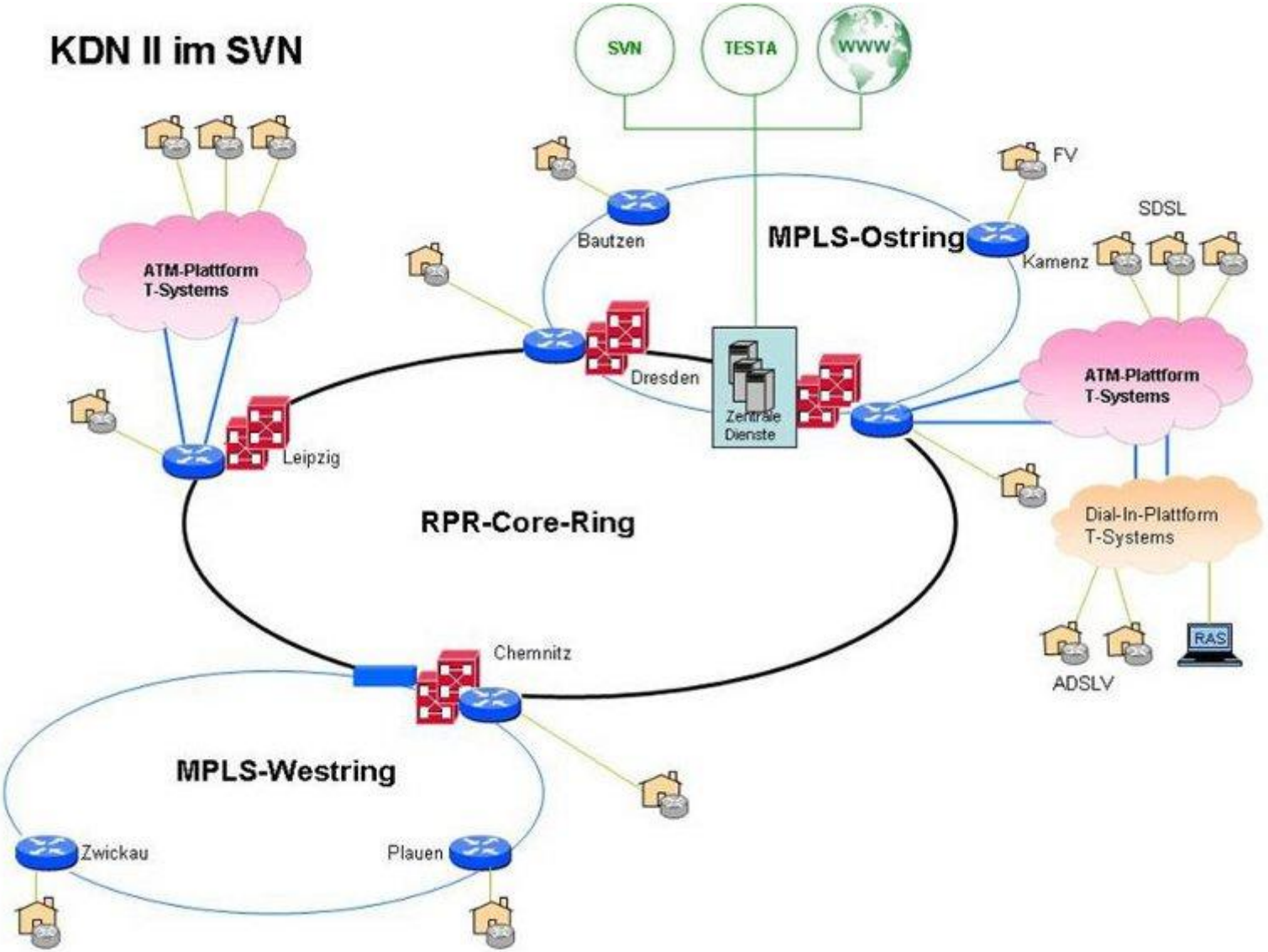
Quelle: Weichert, Big Data und Datenschutz, 2013

Informationssicherheit

Empfehlungen zur Umsetzung

- Orientierung an BSI-GS, auch wenn, anders als für staatliche Behörden (§ 9 Abs. 2 S. 3 SächsEGovG), für TdS nicht vorgeschrieben
  - Schaffung organisatorischer Grundlagen (Leitlinie, Beauftragter für IS etc.)
  - Entwicklung Sicherheitskonzept gem. IT-GS Vorgehensweise
  - Umsetzung durch Beseitigung vorhandener Schwachstellen und Einführung der im Konzept vorgesehenen Maßnahmen
  - Aufrechterhaltung und Verbesserung durch Prüfung Konzepte und Maßnahmen

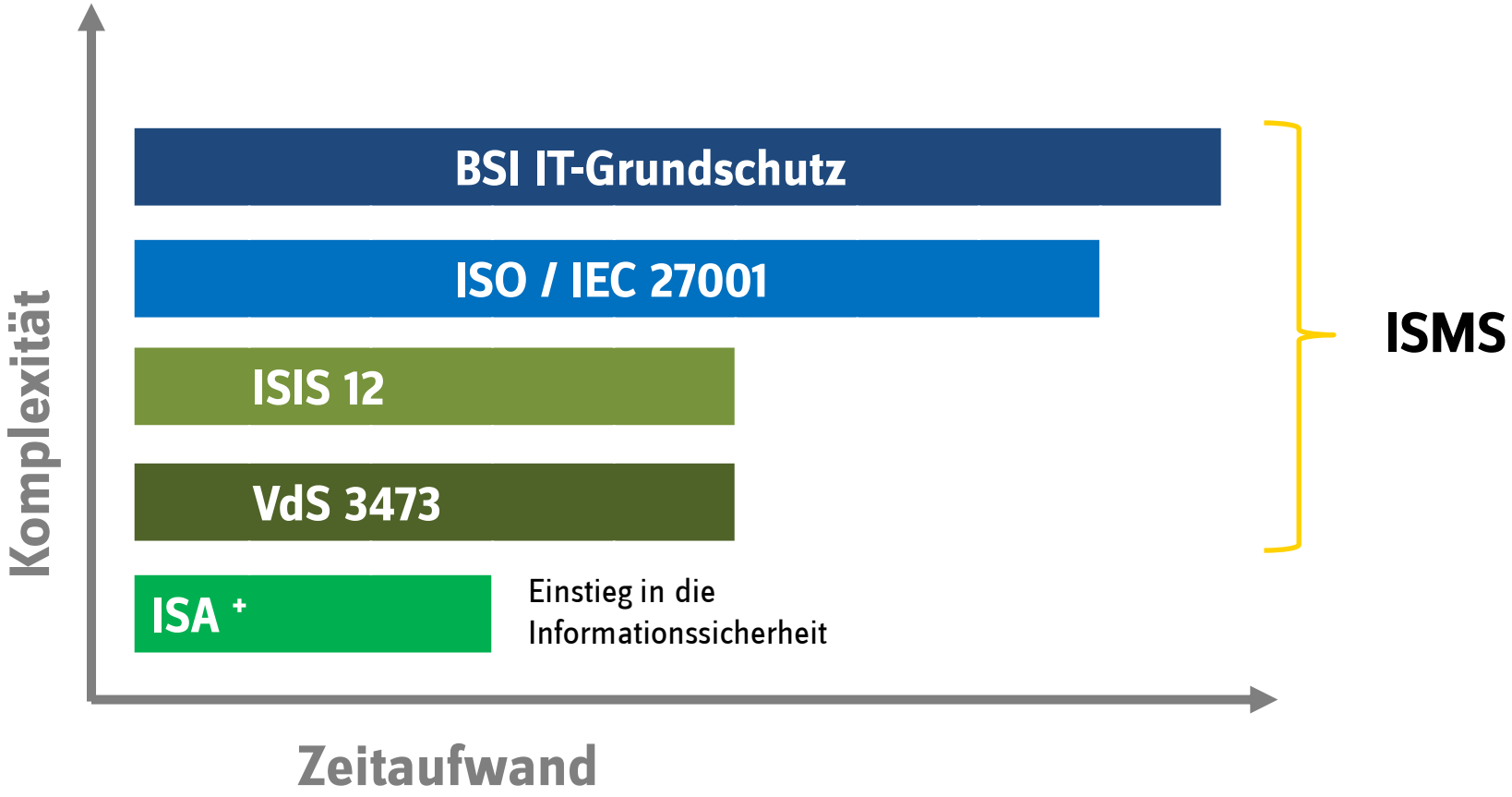
- Parallel Durchsetzung von Sofortmaßnahmen
  - Anschluss an das KDN
  - Umstellung auf Zertifikate der Sachsen Global CA
  - E-Mail-Verschlüsselung einsetzen



Quelle: http://www.kdn-sachsen.de/kdn/idx.asp

Informationssicherheit

Empfehlungen zur Umsetzung



Quelle: http://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12.html

Informationssicherheit

Leitfäden und Empfehlungen

- SAKD: Musterleitlinie zur Herstellung und Gewährleistung der Informationssicherheit in sächsischen Kommunalverwaltungen (analog VwV Informationssicherheit des FS)
- Leitlinie für die Informationssicherheit in der öffentlichen Verwaltung
- Leitfaden Informationssicherheit des BSI

5 Basiskomponenten

Basiskomponenten

Rechtsgrundlage

Frist: 9.8.2014

§ 10 Abs. 3 SächsEGovG:

„Die staatlichen Behörden sind verpflichtet, diejenigen Daten elektronisch zur Verfügung zu stellen und mindestens einmal jährlich zu aktualisieren, die für den Betrieb der im Freistaat Sachsen als **Zuständigkeitsfinder eingesetzten Basiskomponente** notwendig sind. Zu diesen Daten zählen insbesondere die Stammdaten der jeweiligen Behörde und elektronische Verweisungen auf die von der jeweiligen Behörde über öffentlich zugängliche Netze schon bereitgestellten elektronischen Formulare."

§ 14 Abs. 2 SächsEGovG:

„§ 10 Abs. 3 gilt für die Träger der Selbstverwaltung entsprechend. Die Vorgaben der Rechtsverordnungen gemäß § 10 Abs. 4 Satz 3 und 4 gelten auch für die Träger der Selbstverwaltung, **soweit** sie Basiskomponenten nutzen oder gemäß Satz 1 in Verbindung mit § 10 Abs. 3 zur Bereitstellung elektronischer Daten verpflichtet sind."

Der IT-Kooperationsrat beschließt, soweit kommunale Belange berührt werden, Empfehlungen für die Kommunen und die staatlichen Behörden insbesondere zu… 6. der Festlegung der … elektronisch zu liefernden Daten für die im Freistaat Sachsen als Zuständigkeitsfinder eingesetzte Basiskomponente …" **(§ 18 Abs. 3)**

Basiskomponenten

Rechtsgrundlage (Forts.)

§ 14 Abs. 1 Satz 1,2 SächsEGovG:

Die in § 10 Abs. 1 Satz 4 und 5 benannten Behörden **können Basiskomponenten auch den Trägern der Selbstverwaltung zur Verfügung stellen**. Die im Freistaat Sachsen als Zuständigkeitsfinder eingesetzte Basiskomponente gemäß § 10 Abs. 3 wird den Trägern der Selbstverwaltung zur Verfügung gestellt..“

§ 10 Abs. 4 S.3 , 4 SächsEGovG:

„Die Staatsregierung wird ferner ermächtigt, die Ausgestaltung einzelner Basiskomponenten unter dem Vorbehalt der Bereitstellung von Haushaltsmitteln für die Umsetzung durch den Landtag jeweils durch **Rechtsverordnung** zu regeln. Die Rechtsverordnungen nach Satz 3 können insbesondere Regelungen ent-halten über… (Zuständigkeitsfinder, Interoperabilitäts- und Informationssicherheitsstandards, sorbische Sprache, die von der konkreten Basiskomponente zu verarbeitenden personenbezogenen Daten)…“

Nutzungsvereinbarung vom 20.8.2014 i.V.m. § 29a Sächs FAG, Laufzeit bis Ende 2018

„„Für die Nutzung der e-Government-Basiskomponenten des Freistaates Sachsen beteiligen sich die Kommunen an den Betriebs- und Personalkosten. Der Finanzierungsbeitrag an den Betriebs- und Personalkosten beträgt in den Jahren 2015 bis 2018 jeweils 404 000 Euro. Im Jahr 2016 wird überprüft, ob eine Anpassung des Finanzierungsbeitrages für die Jahre 2017 und 2018 notwendig ist.“

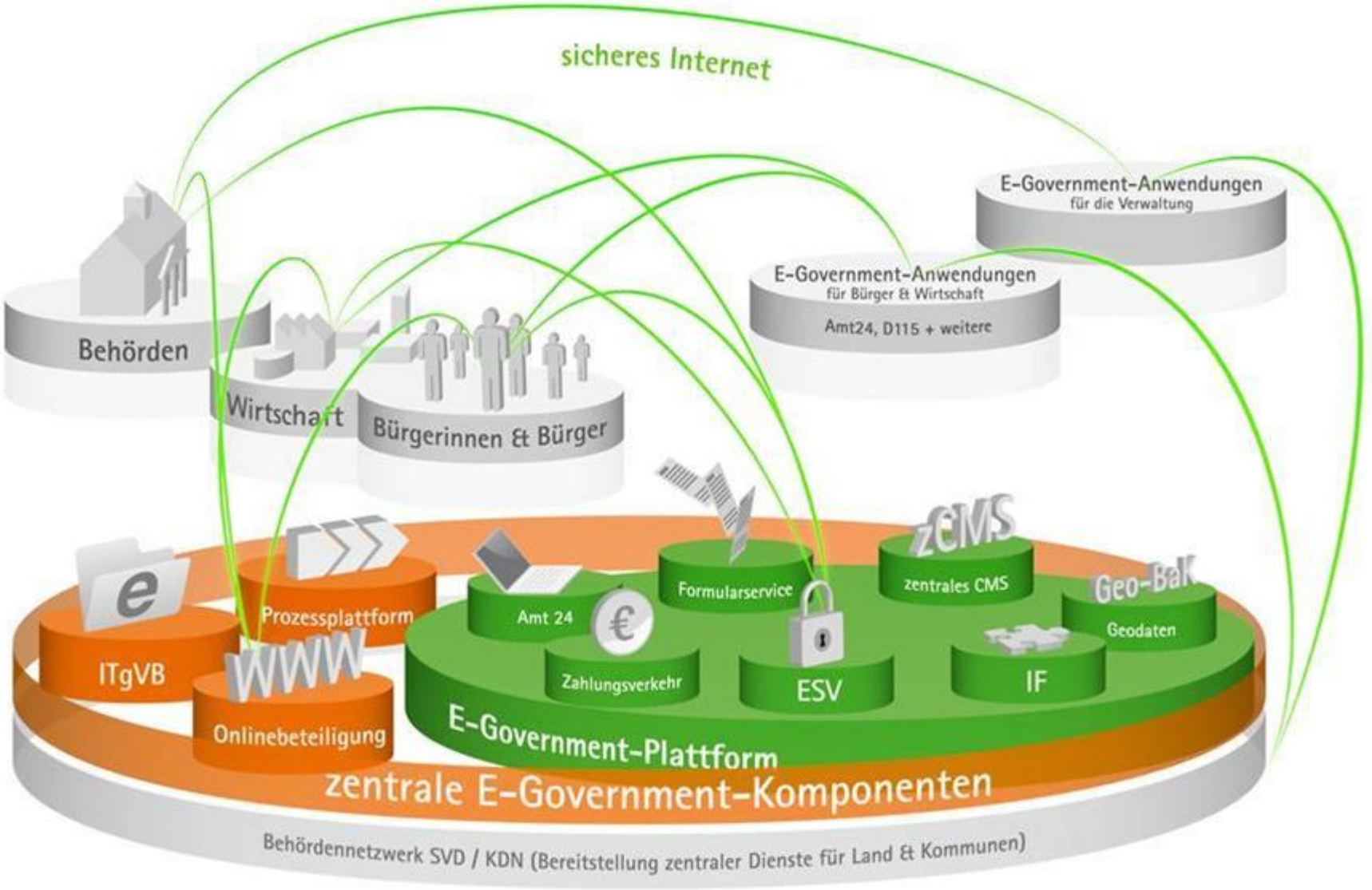
Basiskomponenten

Hintergrund

Schaffung von zentralen E-Government-Komponenten zur Nutzung von staatlichen Behörden und Trägern der Selbstverwaltung in Sachsen

- Basiskomponenten - Gegenstand der Nutzungsvereinbarung
  - Amt24 (Service-Portal der sächsischen Verwaltungen mit Informationen zu Verwaltungsverfahren, Online-Diensten und zuständigen Behörden)
  - Formularservice (verwaltungsübergreifende Entw. und Verwendung elektr. Formulare)
  - Zentrales Content Management System (Erfassen, Verw. und Publ. von Behördeninfo.)
  - Geodaten
  - Zahlungsverkehr
  - Elektronische Signatur und Verschlüsselung
  - Prozessplattform
  - Beteiligungsportal

- Weitere BaK möglich



Quelle: http://www.egovernment.sachsen.de/993.html

Basiskomponenten

Inhalt

Pflichten der TdS betreffend Basiskomponenten

- Pflicht zur Bereitstellung von Daten für BaK „Zuständigkeitsfinder“ (§ 14 Abs.2 S.1 i.V.m. § 10 Abs. 3)
- *Soweit*-Pflicht: TdS müssen sich an die Vorgaben halten, die durch VO vorgegeben werden können, soweit sie BaK nutzen (§ 14 Abs.2 S.2 i.V.m. § 10 Abs. 4 S.3, 4).

  „Die Vorgaben der Rechtsverordnungen gemäß § 10 Abs. 4 Satz 3 und 4 gelten auch für die Träger der Selbstverwaltung, soweit sie Basiskomponenten nutzen oder gemäß Satz 1 in Verbindung mit § 10 Abs. 3 zur Bereitstellung elektronischer Daten verpflichtet sind.“

- Rechtsverordnungen zu BaK sind in Planung.

Basiskomponenten

Inhalt (Forts.)

Rechte, Optionen und Möglichkeiten der TdS betreffend Basiskomponenten

- BaK Zuständigkeitsfinder wird den TdS zur Verfügung gestellt (§ 14 Abs. 1 S. 2).
- Nutzungsberechtigung der TdS betr. BaK gemäß Nutzungsvereinbarung vom 20.8.2014
- Im übrigen „können“ BaK den TdS zur Verfügung gestellt werden (§ 14 Abs. 1 S. 1)

Basiskomponenten

Empfehlungen zur Umsetzung

Nutzung im Rahmen der Nutzungsvereinbarung zur Verfügung gestellter BaK bei Identifizierung von Lösungen für SächsEGovG – Anforderungen

- Kontaktstelle BaK (u.a. SID, SAKD)
- vgl. auch Dokument „Handreichung für zuständige Stellen zum Einsatz der E-Government-Basiskomponenten, Version 1.2 vom 08.10.2009“

Vielen Dank

Dierk Schlosshan
Rechtsanwalt

eureos gmbh steuerberatungsgesellschaft
rechtsanwaltsgesellschaft

Telefon: + 49 / 351 / 4976 1519
d.schlosshan@eureos.de
→ **www.eureos.de**

eureos