Information Security Society Switzerland

SuisseID – Risiken und Haftungsfragen

ISSS Security Lunch
SuisseID - Identitätsmissbrauch

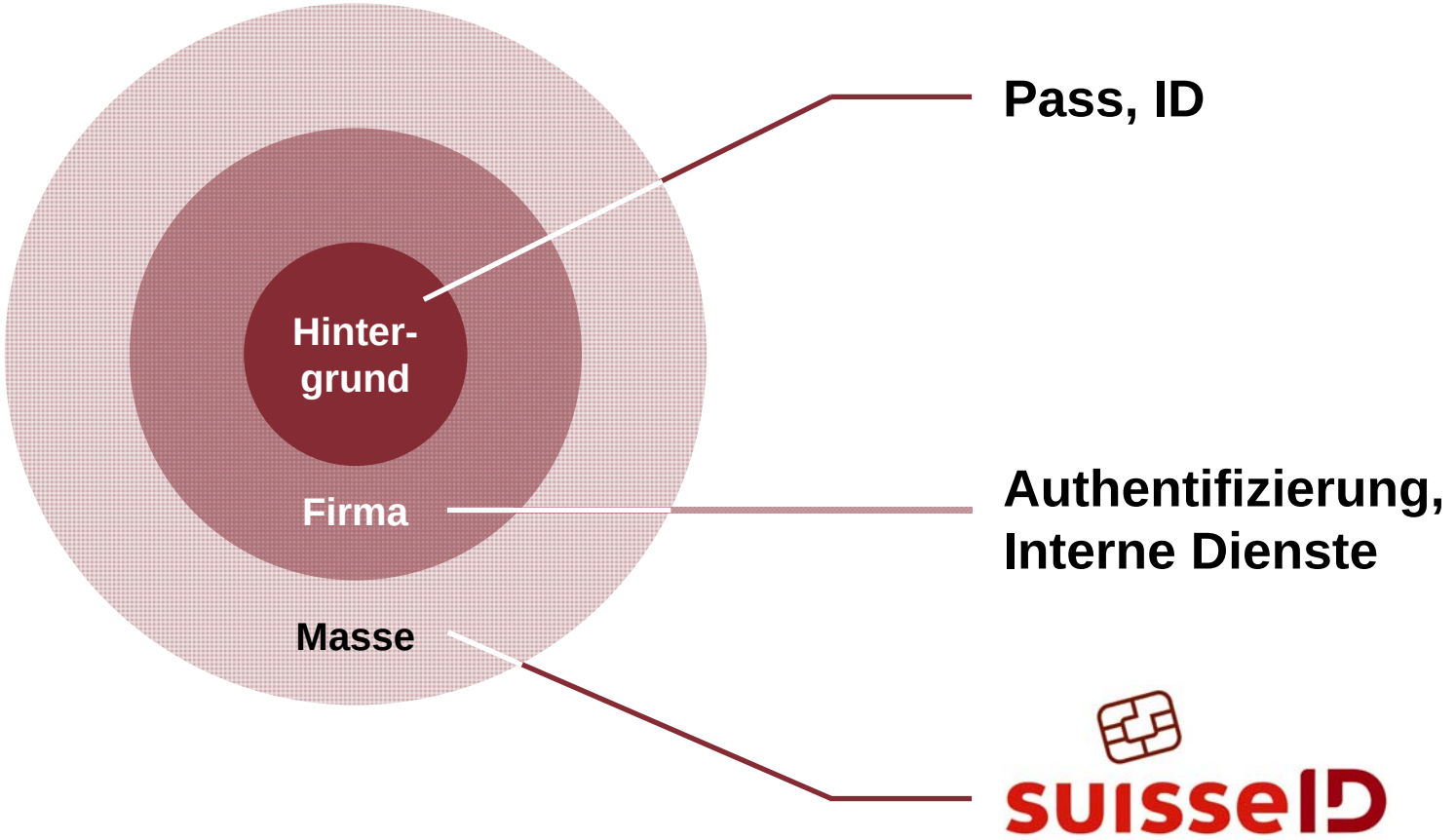
28. Juni 2011, 12:00 - 14:00, Schmiedstube, Bern

Samuel Klaus, Dr.iur., Rechtsanwalt
Walder Wyss AG

Übersicht

1. Zertifizierungsdienste / PKI
2. Definition / Begrifflichkeiten
3. Anwendungsmöglichkeiten
4. Digitale Signatur: Normalfall / Missbrauchsfall
5. Problembereiche
6. Haftungsnormen
7. Ansprüche
8. OR 59a: Voraussetzungen / Folgen
9. ZertEs 16: Voraussetzungen / Folgen
10. Zusammenfassung / Fazit

1. Zertifizierungsdienste / PKI *



* Public Key Infrastructure

2. Definition / Begrifflichkeiten

≠ **ZertES ***

≠ **Digitale Signatur (OR 14.2bis)**

= **Marke des SECO, lizenziert an: ****

- QuoVadis Trustlink Schweiz AG
- Die Schweizerische Post
- Swisscom (Schweiz) AG

* BG über die elektronische Signatur, SR 943.03
** Marken Nr. 596114, 59755/2010, www.swissreg.ch

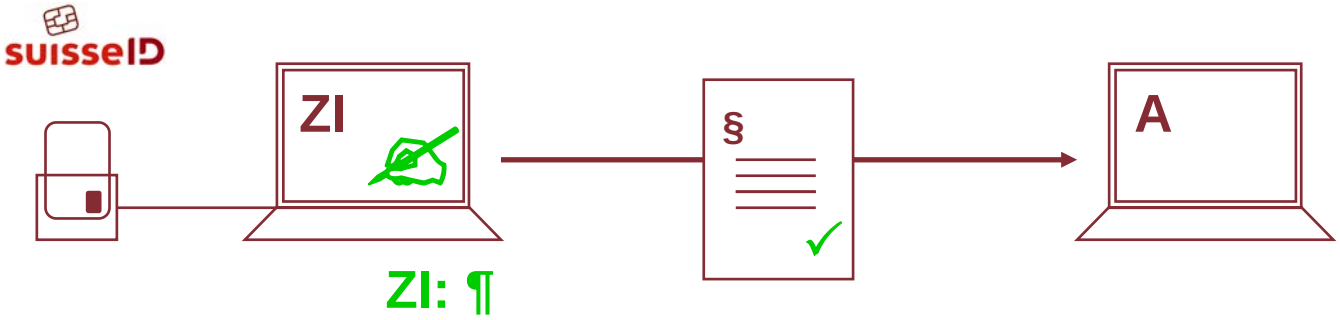
3. Anwendungsmöglichkeiten

Authentifizierung

Digitale Signatur (OR 14.2bis)

Indirekte Anwendungen
(z.B. E-Mail Verschlüsselung)

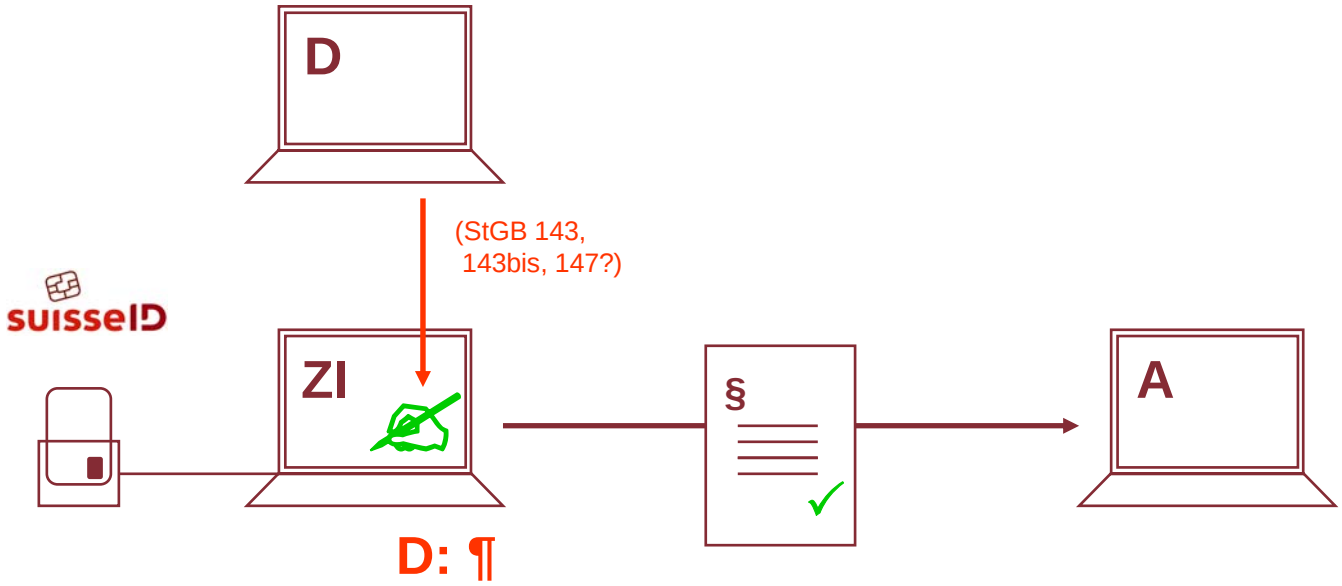
4.1 Digitale Signatur - Normalfall



1	2	3	4
SuisseID	**Signierung durch Zertifikatsinhaber**	**Gültige qualifizierte elektronische Signatur gem. OR 14.2bis**	**Empfang durch « Akzeptor »**

ZI = Zertifikatsinhaber («Anwender»)
A = Akzeptor (z.B. Diensteanbieter)

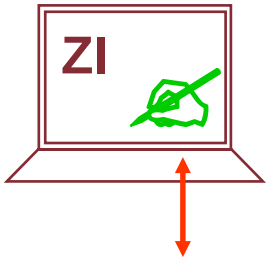
4.2 Digitale Signatur - Missbrauchsfall

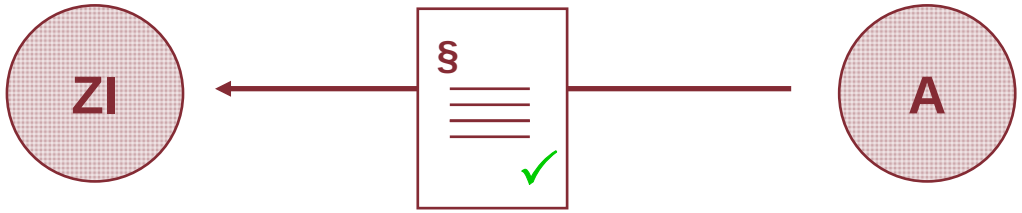


1	2	3	4
SuisseID	**Signierung durch Dritten, ohne Wissen und Mitwirkung des Zertifikatsinhabers**	**Gültige qualifizierte elektronische Signatur gem. OR 14.2bis**	**Empfang durch « Akzeptor »**

ZI = Zertifikatsinhaber («Anwender»)
A = Akzeptor (z.B. Diensteanbieter)
D = Dritter («Angreifer»)

5 Problembereiche





Willenserklärung

tatsächlicher Wille

Beweislast ?

Haftung ?

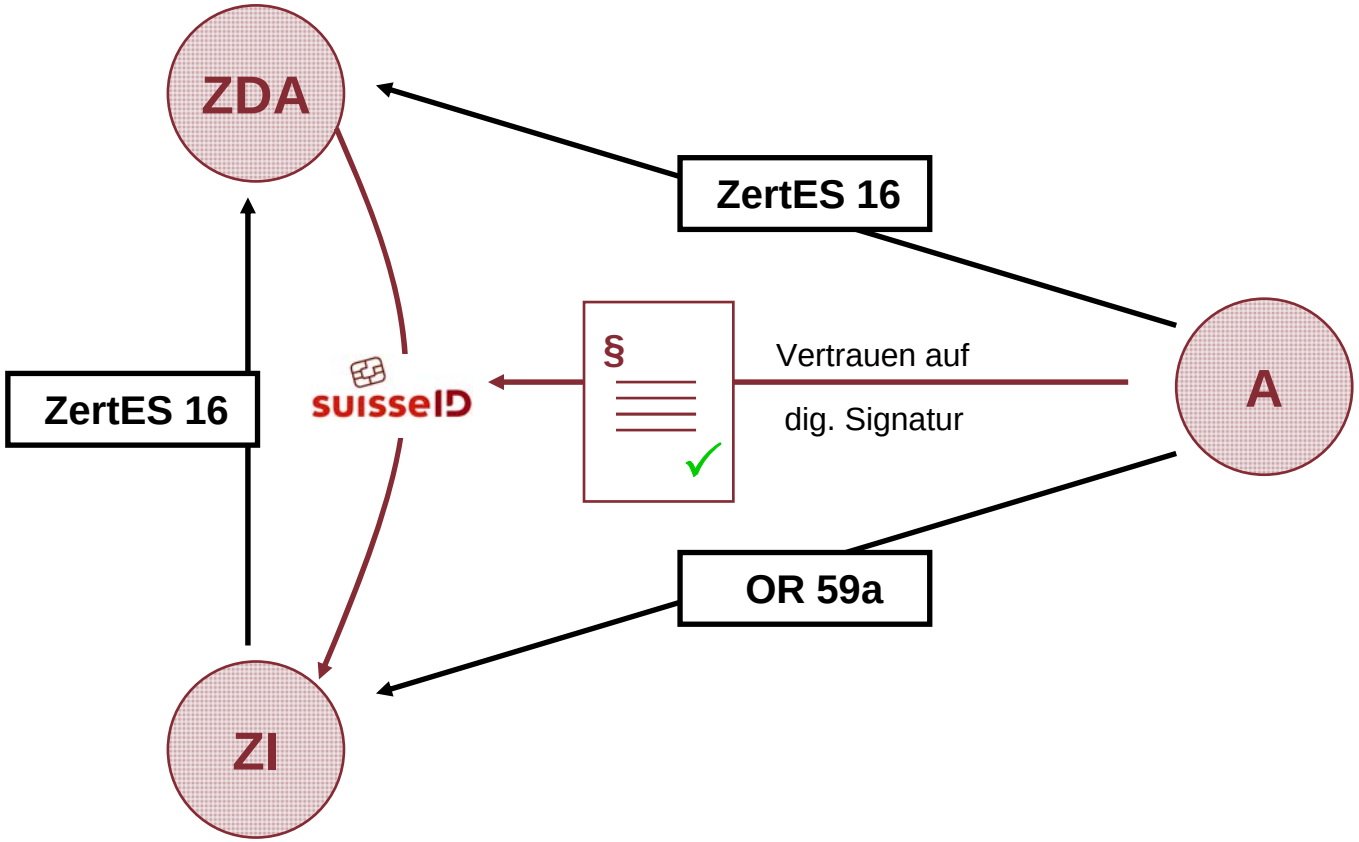
Rechtssicherheit ?

Vertragserfüllung ?

Schadenersatz ?

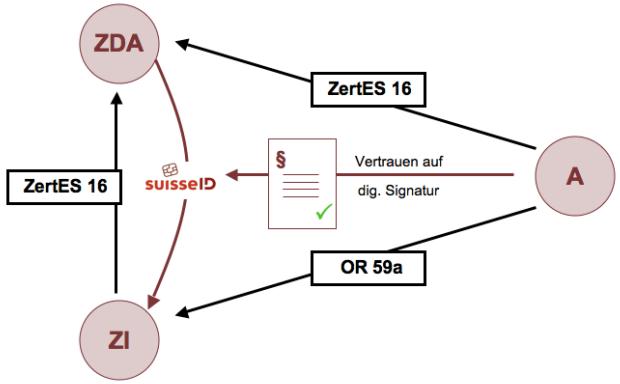
ZI = Zertifikatsinhaber («Anwender»)
A = Akzeptor (z.B. Diensteanbieter)
D = Dritter («Angreifer»)

6 Haftungsnormen



ZDA = Zertifizierungsdienste-Anbieter
ZI = Zertifikatsinhaber («Anwender»)
A = Akzeptor (z.B. Diensteanbieter)

7 Ansprüche

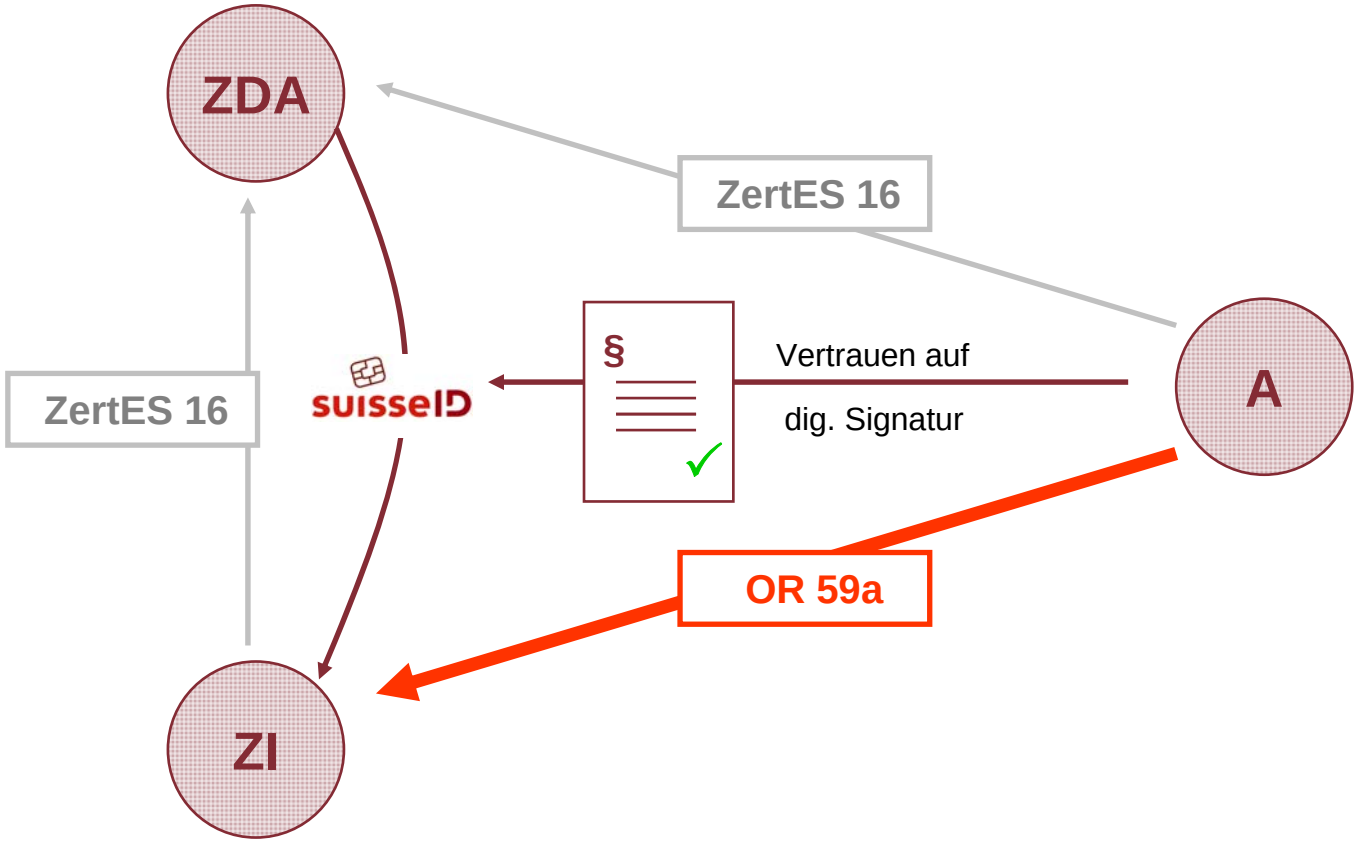


Anspruch auf Schadenersatz	Von A (Akzeptor)	Von ZI (Zert.Inhaber)
Gegen ZI	OR 59a (iVm VZertES 11)	- -
Gegen ZDA	ZertES 16 iVm ZertES 6.2.c	ZertES 16 iVm ZertES 6.2.c

ZertES: BG über die elektronische Signatur, SR 943.03
VZertES: Verordnung über die elektronische Signatur, SR 942.032

ZDA = Zertifizierungsdienste-Anbieter
ZI = Zertifikatsinhaber («Anwender»)
A = Akzeptor (z.B. Diensteanbieter)

8.1 OR 59a



ZDA = Zertifizierungsdienste-Anbieter
ZI = Zertifikatsinhaber («Anwender»)
A = Akzeptor (z.B. Diensteanbieter)

8.2 OR 59a: Voraussetzungen

Haftung des ZI nach OR 59a (iVm VZertES 11) :

OR 59a

[1] Der Inhaber eines Signaturschlüssels haftet Drittpersonen für Schäden, die diese erleiden, weil sie sich auf das qualifizierte gültige Zertifikat einer anerkannten Anbieterin von Zertifizierungsdiensten im Sinne des ZertES verlassen haben.

[2] Die Haftung entfällt, wenn der Inhaber des Signaturschlüssels glaubhaft darlegen kann, dass er die nach den Umständen notwendigen und zumutbaren Sicherheitsvorkehrungen getroffen hat, um den Missbrauch des Signaturschlüssels zu verhindern.

[3] Der Bundesrat umschreibt die Sicherheits-vorkehrungen im Sinne von Absatz 2. → **VZertES 11**

Schlauri, Elektronische Signaturen (2002) :

[746] *Kontrolle des Halters über den Signierschlüssel*: Der Zertifizierungsdiensteanbieter hat zu überprüfen, ob der Schlüsselhalter über eine sichere Signiereinheit verfügt [...]. Kommt dennoch ein **unsicheres Gerät** zum Einsatz, haftet der Schlüsselhalter jedenfalls nach Art. 59a [OR].

(Ebenso: BK-Brehm, OR 59a, Rz 6)

BK-Brehm, OR 59a (2006) zu VZertEs 11:

[19] Art. 11 führt einige Sicherheitsvorkehrungen des Inhaber eines Signaturschlüssels auf [...].

[20] Diese Pflichten sind nicht ausschöpfend aufgeführt. Eine Haftung des Inhabers kann auch aus **anderen, allgemeinen Pflichtverletzungen** entstehen [...].

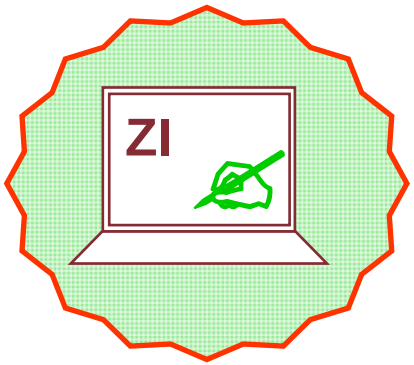
8.3 OR 59a: Folgen

Haftungsfolgen und Unsicherheit für Zertifikateinhaber (ZI) :

(in heutiger Form)

= « unsicheres Gerät » = Haftung OR 59a

(zug. A)



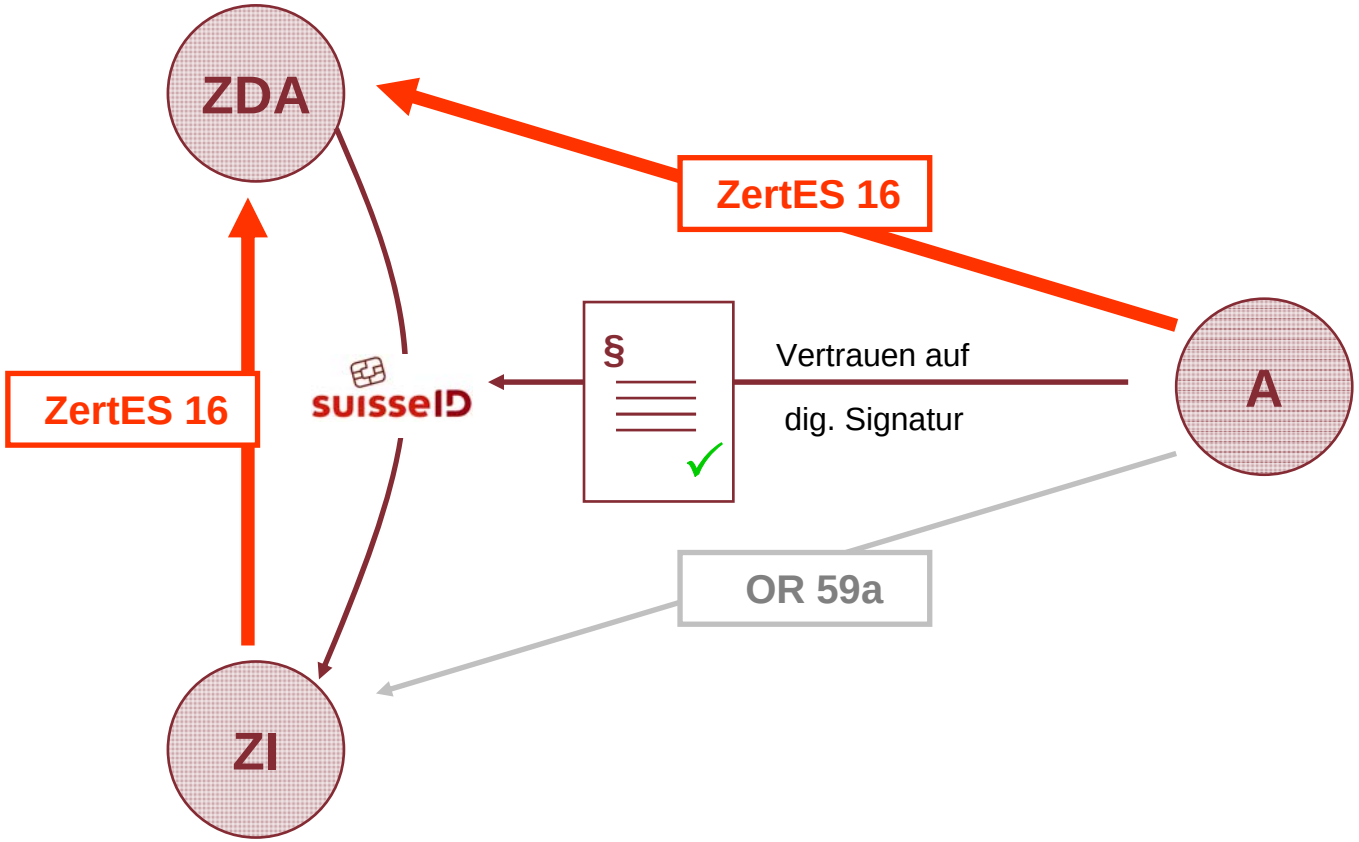
Schutz der Arbeitsumgebung

= « allgemeine Sorgfaltspflicht » = Unklarer Begriff *

* www.melani.admin.ch/themen/00166/index.html

ZI = Zertifikatsinhaber («Anwender»)
A = Akzeptor (z.B. Diensteanbieter)

9.1 ZertES 16



ZDA = Zertifizierungsdienste-Anbieter
ZI = Zertifikatsinhaber («Anwender»)
A = Akzeptor (z.B. Diensteanbieter)

9.2 ZertES 16: Voraussetzungen

Haftung des ZDA nach ZertES 16 iVm ZertES 6.2.c :

ZertES 16

[1] Die Anbieterin von Zertifizierungsdiensten haftet der Inhaberin oder dem Inhaber des Signaturschlüssels und Drittpersonen, die sich auf ein gültiges qualfiziertes Zertifikat verlassen haben, für Schäden, die diese erleiden, weil die Anbieterin den Pflichten aus diesem Gesetz und den entsprechenden Ausführungsvorschriften nicht nachgekommen ist.

[2] Sie trägt die Beweislast dafür, den Pflichten aus diesem Gesetz und den Ausführungsvorschriften nachgekommen zu sein.

[3] Sie kann ihre Haftung aus diesem Gesetz weder für sich noch für Hilfspersonen wegbedingen [...].

ZertES 6.2.c :

[2] Die Signaturerstellungseinheiten müssen zumindest gewährleisten, dass die für die Erzeugung der Signatur verwendeten Signaturschlüssel: [...]

c. von der rechtmässigen Inhaberin oder vom rechtmässigen Inhaber vor der missbräuchlichen Verwendung durch andere verlässlich geschützt werden können.

Schlauri, Elektronische Signaturen (2002) :

[746] *Kontrolle des Halters über den Signierschlüssel*: Der Zertifizierungsdiensteanbieter hat zu überprüfen, ob der Schlüsselhalter über eine **sichere Signiereinheit** verfügt.

9.3 ZertES 16: Folgen

Haftungsfolgen für Zertifizierungsdienste-Anbieter (ZDA) :

(in heutiger Form) = « unsicheres Gerät » = Haftung ZertES 16

(zug. A / ZI)

« ...Pflichten aus diesem Gesetz... » = Was gehört alles zu diesen Pflichten ? = Unklarer Begriff

ZDA = Zertifizierungsdienste-Anbieter
ZI = Zertifikatsinhaber («Anwender»)
A = Akzeptor (z.B. Diensteanbieter)

Zusammenfassung

Bei missbräuchlicher Verwendung der SuisseID durch Dritten ergibt sich :

1. Missbräuchlich signierter Vertrag ist nicht gültig (noch keine Gerichtspraxis)
2. Zertifikateinhaber (ZI) haftet Akzeptor (A) nach OR 59a (auf neg.Interesse)
   - ➔ Regress auf Zertifizierungsdienste-Anbieter nach ZertES 16 iVm ZertES 6.2.c
3. Zertifizierungsdienste-Anbieter (ZDA) haftet :
   - 3.1 nach ZertES 16 iVm ZertES 6.2.c (keine Wegbedingung / Einschränkung)
     - ➔ dem Akzeptor (A)
     - ➔ dem Zertifikateinhaber (ZI)
   - 3.2 aus vertraglichem Grundverhältnis
     - ➔ dem Zertifikateinhaber (ZI)

Fazit

- Risiken und (offene) Haftungsfragen bestehen
- Noch keine Gerichtspraxis
- **Vor SuisseID-Einsatz :**

  → **Individuelle Kosten/Nutzen - Abwägung**