Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

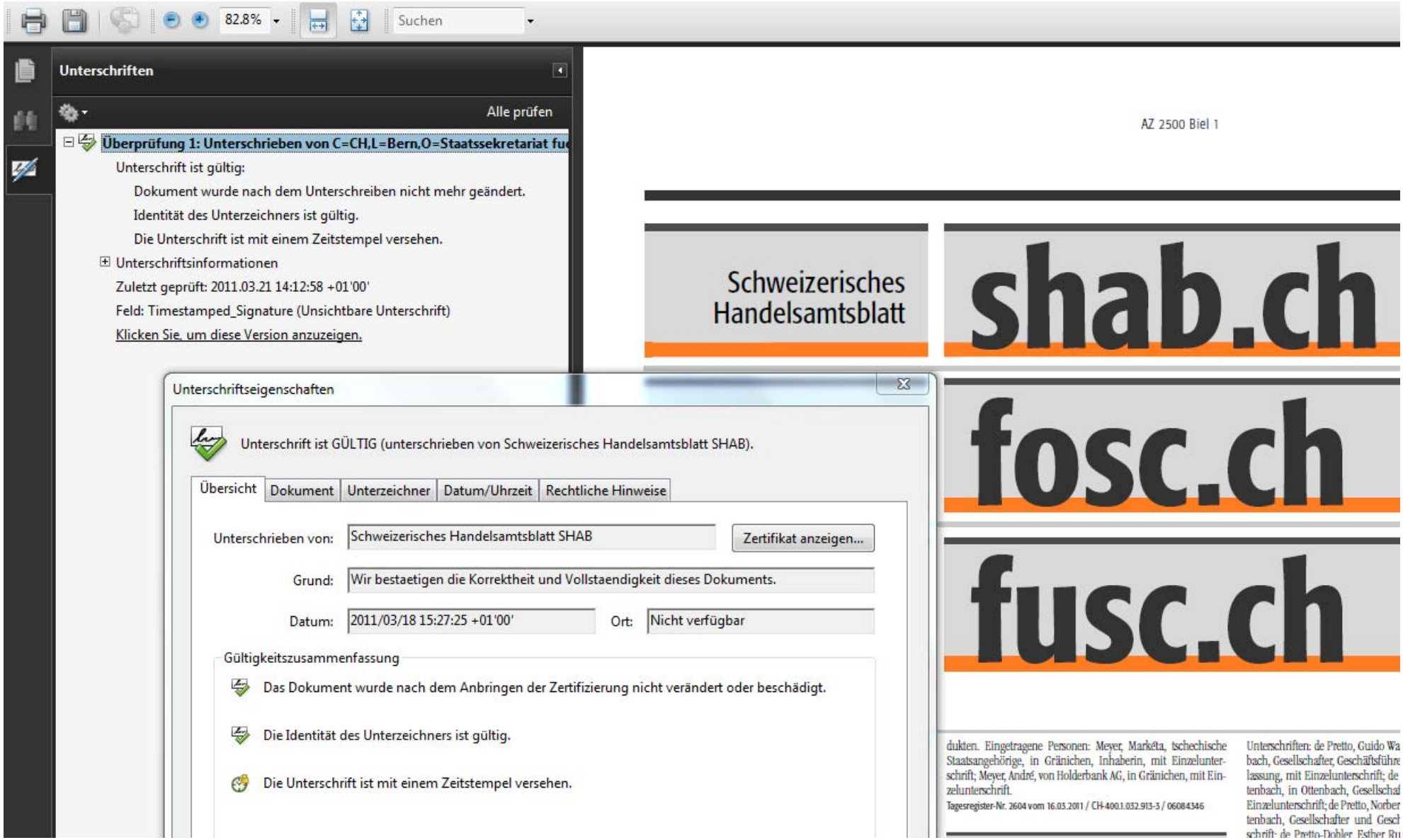
Eidgenössisches Finanzdepartement EFD
Bundesamt für Informatik und Telekommunikation BIT

Das elektronische SHAB-Archiv

Ist das Problem der kryptographischen Langzeitsicherheit gelöst?

29. März 2011

Um was geht es?



Inhalt und Ziel

- Projekt-Anforderungen *(Markwalder)*
- Rechtliche Ausgangslage *(Markwalder)*
- Technische Ausgangslage *(Isler)*
- Lösung *(Isler)*
- Zusammenfassung und Ausblick *(Markwalder)*

Anforderungen des Projekts

- Paradigmenwechsel beim Schweizerischen Handelsamtsblatt
- Archivierungsauftrag der Nationalbibliothek
- Herausforderung Beständigkeit
- Projektauftrag: Konservierung der Form

Rechtliche Ausgangslage

- GeBüV
- ElDI-V
- Freie Beweiswürdigung (kein gesetzlicher Beweiswert)
- Art. 178 ZPO *„Die Partei, die sich auf eine Urkunde beruft, hat deren Echtheit zu beweisen, sofern die Echtheit von der andern Partei bestritten wird; die Bestreitung muss ausreichend begründet werden.“*

- Fragen an die Sachverständigen:
  - Wie sicher ist es, dass Nachricht seit einem bestimmten Zeitpunkt nicht verändert wurde?
  - Allenfalls: Von wem stammt das Dokument? Wer hat es „versiegelt“?

Rechtliche Ausgangslage

- Anforderungen
  - GeBüV konforme Archivierung von signierten PDF Dokumenten
  - Aufbewahrung über einen längeren Zeitraum (mehr als 10 Jahre)
- Art. 9 GeBüV:

Art. 9 Zulässige Informationsträger

[1] Zur Aufbewahrung von Unterlagen sind zulässig:

a. unveränderbare Informationsträger, namentlich Papier, Bildträger und unveränderbare Datenträger;

b. veränderbare Informationsträger, wenn:

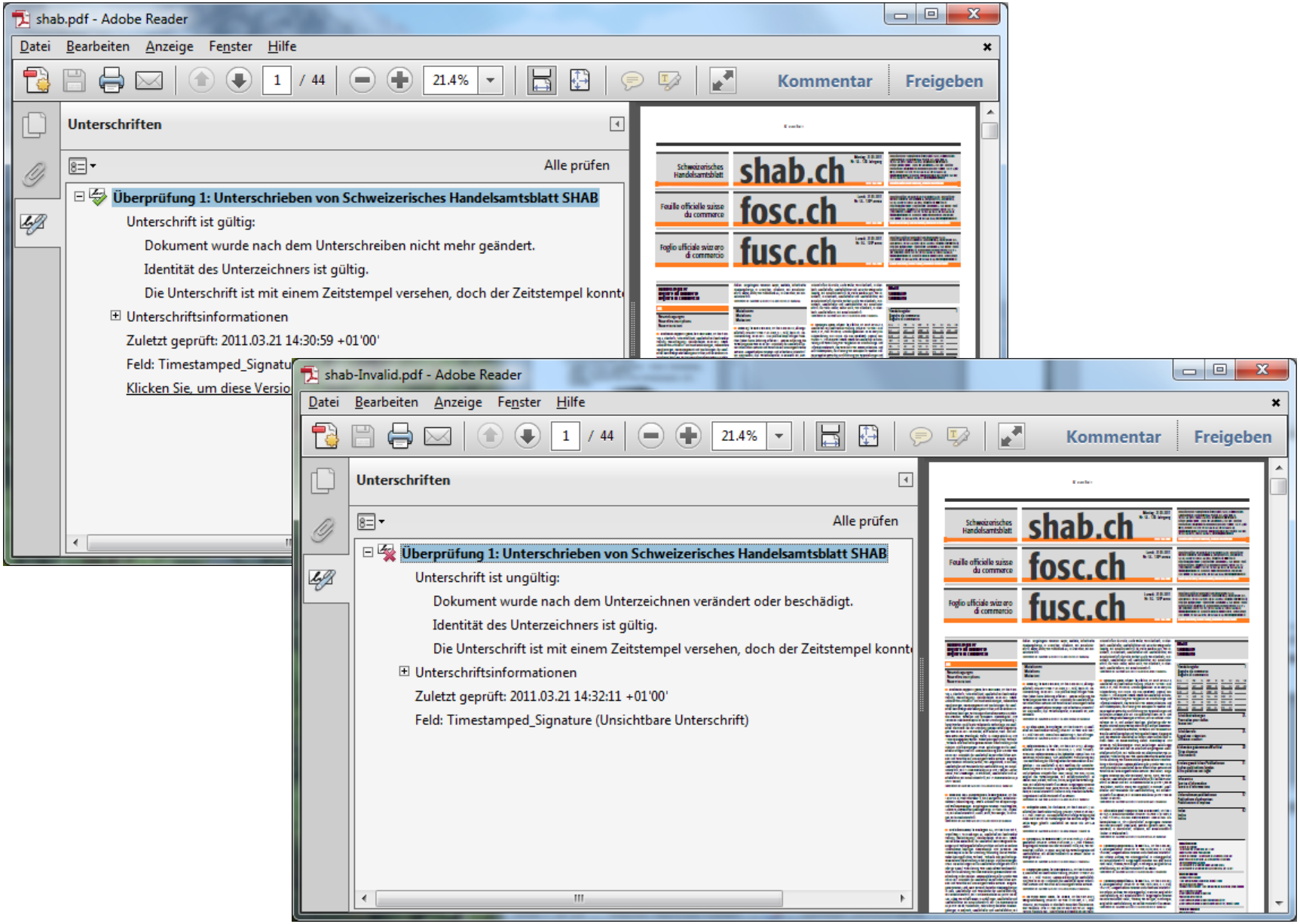
1. technische Verfahren zur Anwendung kommen, welche die Integrität der gespeicherten Informationen gewährleisten (z.B. digitale Signaturverfahren),
2. der Zeitpunkt der Speicherung der Informationen unverfälschbar nachweisbar ist (z.B. durch «Zeitstempel»),
3. die zum Zeitpunkt der Speicherung bestehenden weiteren Vorschriften über den Einsatz der betreffenden technischen Verfahren eingehalten werden, und
4. die Abläufe und Verfahren zu deren Einsatz festgelegt und dokumentiert sowie die entsprechenden Hilfsinformationen (wie Protokolle und Log files) ebenfalls aufbewahrt werden.

Technische Ausgangslage

- Digitale Signatur
  - Gewährleistet die Integrität des Dokuments
  - Mathematische Verknüpfung von einem privaten, kryptografischen Schlüssel mit den zu signierenden Daten

```
SEQUENCE {
  TO BE SIGNED OBJECT
  ...
SEQUENCE {
  OBJECT IDENTIFIER
    sha1withRSAEncryption (1 2 840 113549 1 1 5)
  NULL
  }
  4B 41 98 E7 E6 04 BB DB 20 6B E5 6A F5 82 2A 48
  DB 7F 7B D8 51 04 B0 10 74 6D 62 64 18 83 1B F3
  72 BA A9 24 B3 02 7C 87 BB DF 84 19 E8 8E B2 D0
  3F A9 04 DD C9 7E 2B F6 70 8F 42 E6 40 5E 7C BA
  85 A2 9B AD 61 78 DD F6 E4 31 4F 9C 17 C1 38 AF
  19 3A 86 2A 89 FA 57 0D A4 68 89 96 AB 35 6F FD
  65 6C 5A D1 C0 EF 4F 57 4F 88 C5 F7 74 EA 3F E6
  65 0A 22 88 6B 23 2D A3 A8 05 E5 99 FC 89 21 0A
}
```

Technische Ausgangslage



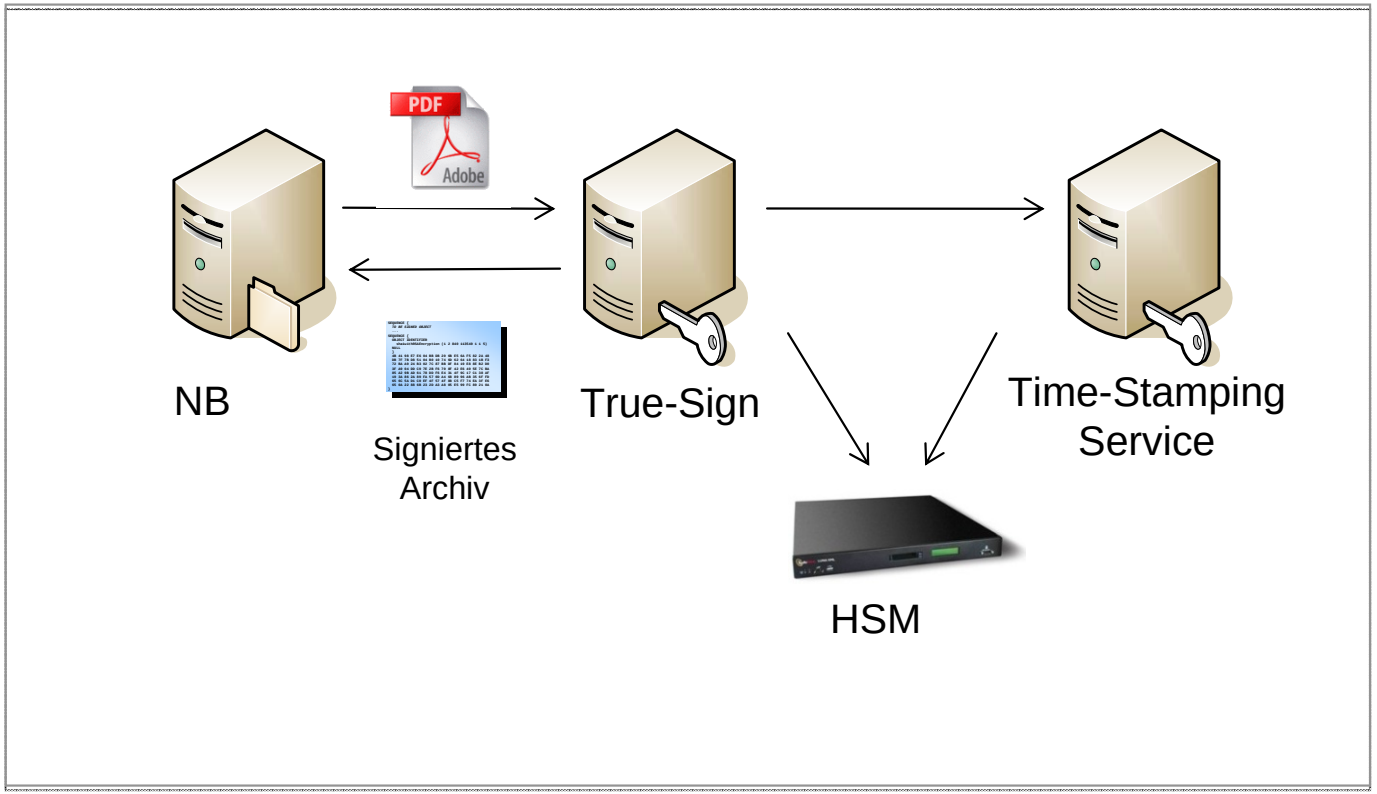
Technische Ausgangslage

- Zeitstempel
  - Gewährleistet dass das Dokument seit dem Zeitpunkt der Speicherung nicht mehr verändert wurde
  - Digitale Signatur
  - Zeitquelle muss vor Manipulation geschützt sein

- Kryptographische Sicherheit
  - Adäquate Wahl der kryptographischen Verfahren (Schlüssellänge, Signatur und Hash Algorithmen)
  - Sicheres Aufbewahren des privaten Schlüsselmaterials (HSM, SmartCard)

Lösung

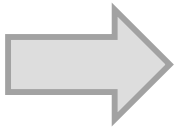
- Einsatz von Digitalen Signaturen
- Verwendung eines internen Zeitstempeldienstes
- Einsatz von Hardware Security Modulen (HSM)



Lösung

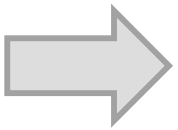
Prozess

1. Einlieferung signiertes PDF von NB
2. Prüfen der Signatur des PDF
3. Erstellen eines Prüfprotokolls



Sicherstellung, dass das PDF zum Zeitpunkt der Einlieferung integer war

4. Signieren und Zeitstempeln des Prüfprotokolls
5. Prüfen der neu erstellten Signatur und des Zeitstempels
6. Erstellen eines Prüfprotokolls



Gewährleistung, dass das PDF zum Zeitpunkt der Einlieferung integer war

Nachhaltigkeit der Lösung

- Ist die Langzeitsicherheit der kryptographischen Verfahren garantiert?
  - Regelmässiges Prüfen der Sicherheit der kryptographischen Verfahren (Hash Algorithmus, Signatur Algorithmus)
  - Regelmässiges Prüfen der Schlüssellängen
  - http://www.keylength.com

Year	Symmetric	Asymmetric		Discrete Logarithm		Elliptic Curve	Hash
		Optimistic	Conservative	Key	Group		
2038	94	1975	2521	187	1975	187	187
2039	94	2012	2582	188	2012	188	188
2040	**95**	**2049**	**2644**	**190**	**2049**	**190**	**190**
2041	96	2086	2707	191	2086	191	191
2042	96	2124	2770	192	2124	192	192

  - SHAB verwendet RSA 4096 und SHA-512
  - Verwenden von Sperrlisten zum Prüfen des Zertifikatsstatus

Nachhaltigkeit der Lösung

- Validierung
  - Periodisches Prüfen des signierten Archivs
  - Systematische Fehler müssen verhindert werden

- Die Lösung ist
  - Wirtschaftlich, effizient
  - Vollständig automatisiert
  - Flexibel für neue Anforderungen

Zusammenfassung

Die Antwort auf die Ausgangsfrage „Ist das Problem der krytographischen Langzeitsicherheit gelöst?“ ist eine juristische Antwort: JA, ABER…

- **JA**, elektronische Dokumente können in einer Art und Weise archiviert werden, dass der Nachweis der Integrität auch nach langer Zeit erbracht werden kann.

- **ABER**, anders als vielleicht bei einem klassischen Archiv ist es keine einmalige Angelegenheit, sondern das Archiv muss gepflegt und die Technologie-Entwicklung muss überwacht werden.

Fragen? Diskussion?

- Herzlichen Dank für Ihre Aufmerksamkeit!