Vertrauensinfrastrukturen: Gütesiegel für Sicherheit und Privatheit

Stefan Schiffner | NIS Expert

Sommerakademie | Kiel| 31. August 2015

European Union Agency for Network and Information Security

ENISA

ENISA

Recommendations

Policy implementation

Supporting Communities

Hands-on

Welcher Service ist Vertrauenswürdig?

Herausforderung

Großes Angebot

Mangel an

- **Info**
- **Zeit**
- **Zugriff**

Man bleibt beim Bewährten

Locked-in-Situation

Behinderung des freien Markts

Politischer Wille dies durch Siegel zu ändern:

Digital Agenda

"review of the European data protection regulatory framework with a view **to enhancing individuals' confidence** [in ICT services] and strengthening their rights[, creating] EU **online trustmarks** for retail websites"

Cybersecurity strategy

"the information available to the public by developing **security labels or kite marks** helping the consumer **navigate the market**."

Amendments for the EU data protection regulation

"In order to **enhance transparency** and compliance with this Regulation, the establishment of certification mechanisms, **data protection seals and marks** should be encouraged"

Was sind diese Siegel

Kennen Sie die?

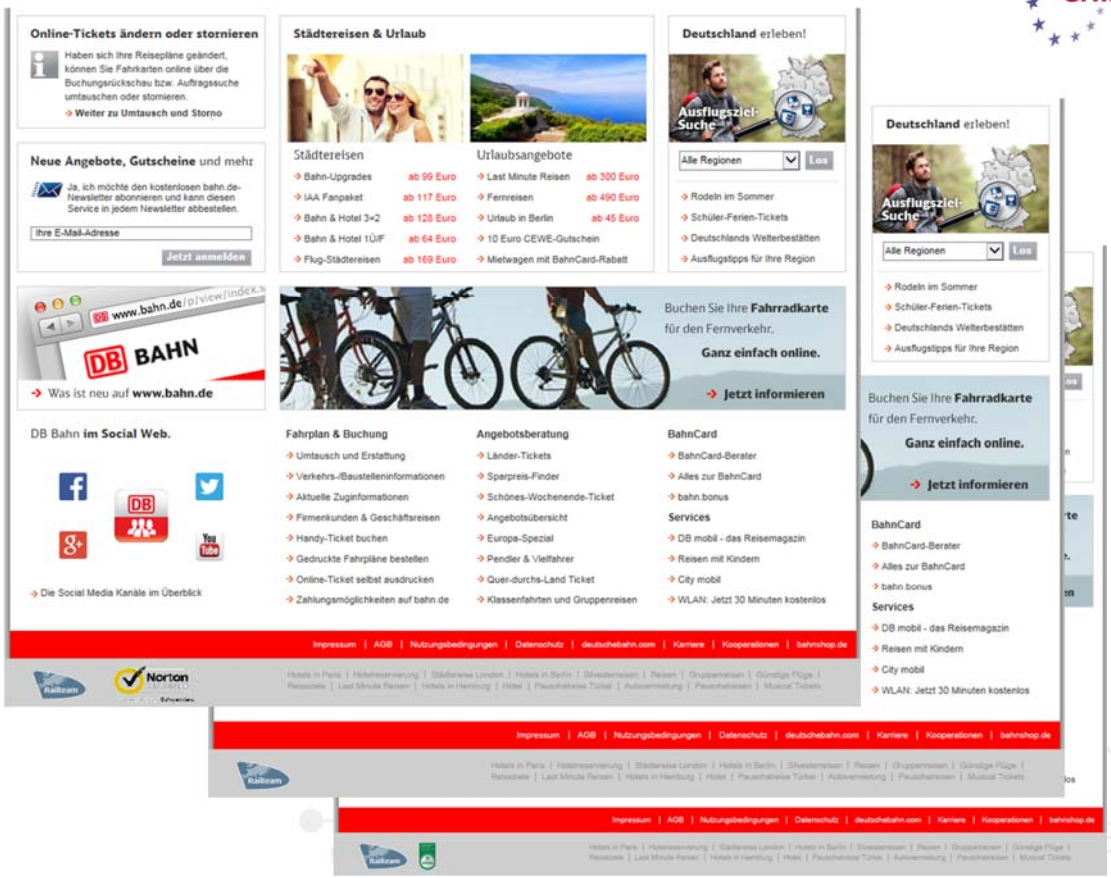
Und nehmen wir mal an Sie kennen all diese Siegel …

Kennen Sie deren Definition?

- Audit-Type (Selbst vs. externe Evaluierung)
- Audit-Gegenstand
- Audit-Häufigkeit

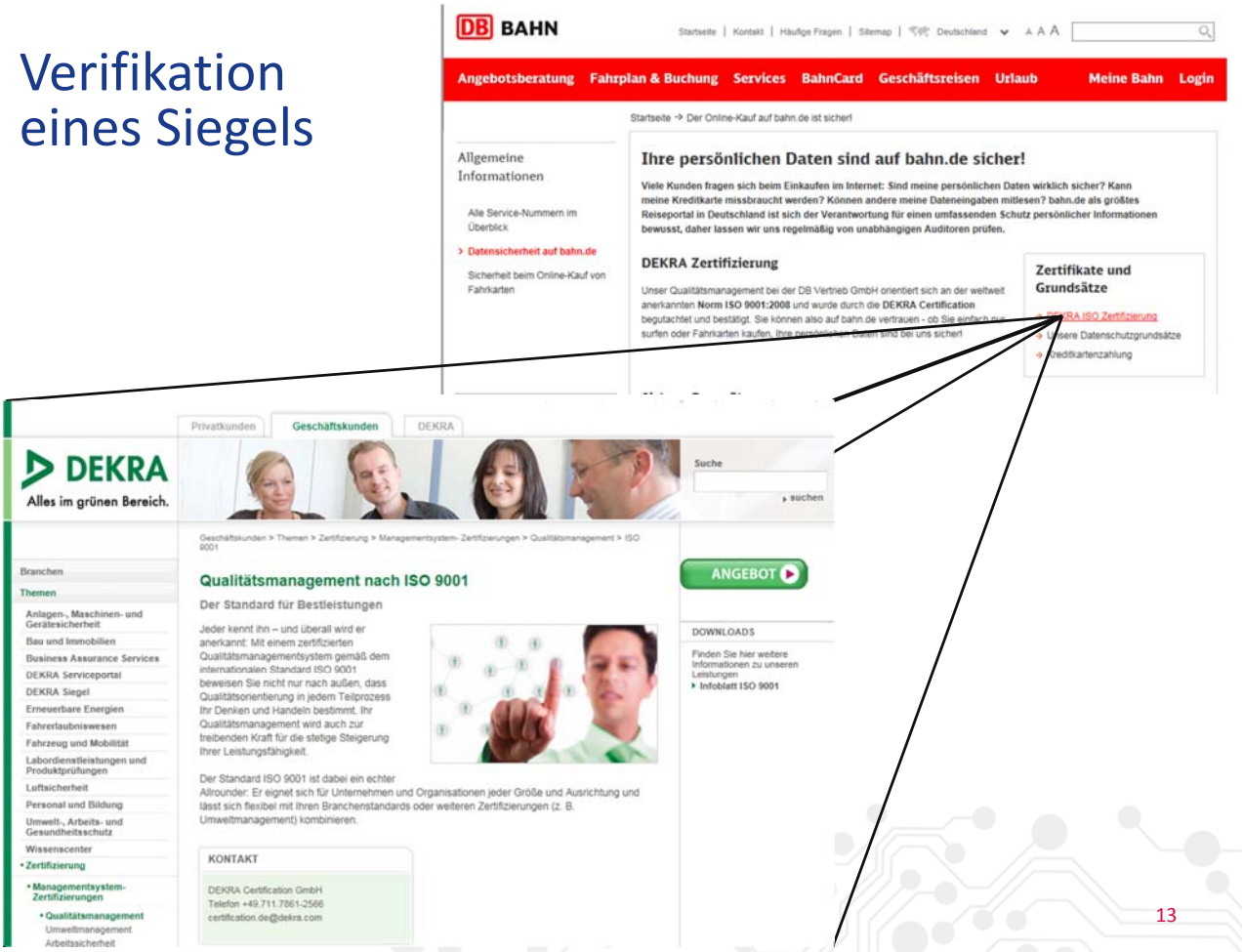
Und dann mal ganz praktisch…

Welcher Seite vertrauen Sie mehr?



Verifikation eines Siegels

Verifikation eines Siegels



Did you ever verify?

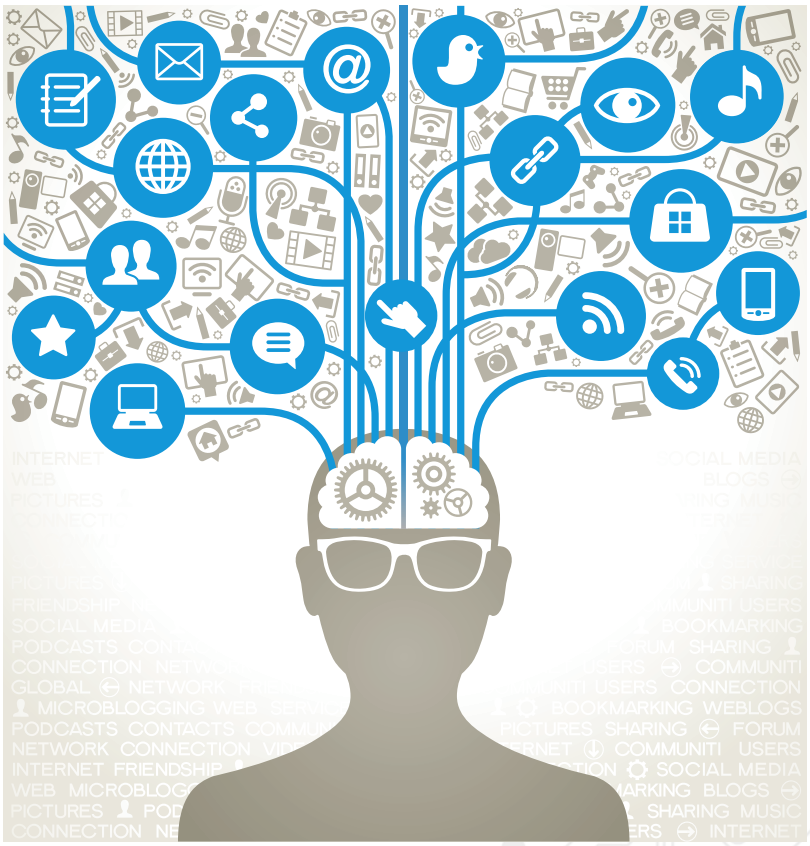
Definition und Beispiel-Instanz eines OSPS

Service publiziert Bewertung
- Graphische Darstellung
- Fälschungssicher
- Negative Bewertungen

Evaluierung → Kommunikation → Validierung

Aussteller Bewertet
- Dritter
- Vordefinierte Kriterien
- Auftraggeber Service

Nutzer prüft OSPS
- Automatisiert
- In Bezug auf eigene Präferenzen
- Ist sich bewusst vom Resultat



Die einzelnen Schritte

Anforderung an die Evaluierung

Herausforderungen

1. Vertrauensverschiebung: Nutzer muss dem Herausgeber des Siegels vertrauen
2. Aussage kraft der Evaluierung
3. Hat der Dienst sich nach der Evaluierung verändert?

Lösungen

1. Common Criteria model, hierarchische Vertrauensmodele, Standards
2. Standards müssen die Serviceart, Datenschutz- und Sicherheitsanforderungen, Evaluationsrichtlinien, und Häufigkeit einschließen
3. Zufallskontrollen, vorbereitende Maßnahmen für Kryptographische Lösungen

Kommunikation

Herausforderungen

1. Bewusstsein
2. Verständnisprobleme btr Vertrauenssignal und Siegel
3. Wahrnehmung
4. Mehrdimensionalität
5. Marktmonopol

Lösungen

1. Bildung und Information
2. Standards
3. Ikonisierung
4. Gesetzgebung sollte Anreize schaffen OSPS zu gebrauchen

Integrität

Herausforderungen

1. (Darstellung der) Siegel sind leicht zu Fälschen
2. Die Verifikationskette kann leicht unterbrochen werden
3. Nutzer machen Fehler bei der Prüfung

Lösungen

1. Kryptographische verfahren für Integrität
   Zertifikate, Signaturen, Hashs
2. Automatisierung

Validierung

Herausforderungen

1. Unwissenheit
2. Unfähigkeit
3. Unvergleichbarkeit

Lösungen

1. Automation
2. Maschinenlesbare Präferenzen

Zusammenfassung

Take home message

Nutzer können Internetdienste nicht bewerten

- Sie bleiben also beim Vertrauten
- Locked-in-Situation
- Monopolbildung (mit allen negativen Folgen)

Online Siegel für Privatheit und Sicherheit werden vom Gesetzgeber diskutiert um diese bedauerliche Situation zu verändern.

Sie werden aber weitestgehend ignoriert

Um wirklich zu funktionieren muss der Prozess optimiert werden.

- Klare Evaluierungsregeln
- Sichere Übertragung (Zertifikate, Signaturen, Hashs)
- Nutzerfreundlichkeit (vor allem durch Automatisierung der Validierung

Wirtschaftliche Anreize sollten genutzt werden um die Verbreitung von OSPS zu fördern.

What is next?
October 7/8
Luxemburg

Annual Privacy Forum