



Vertrauensinfrastrukturen: Gütesiegel für Sicherheit und Privatheit

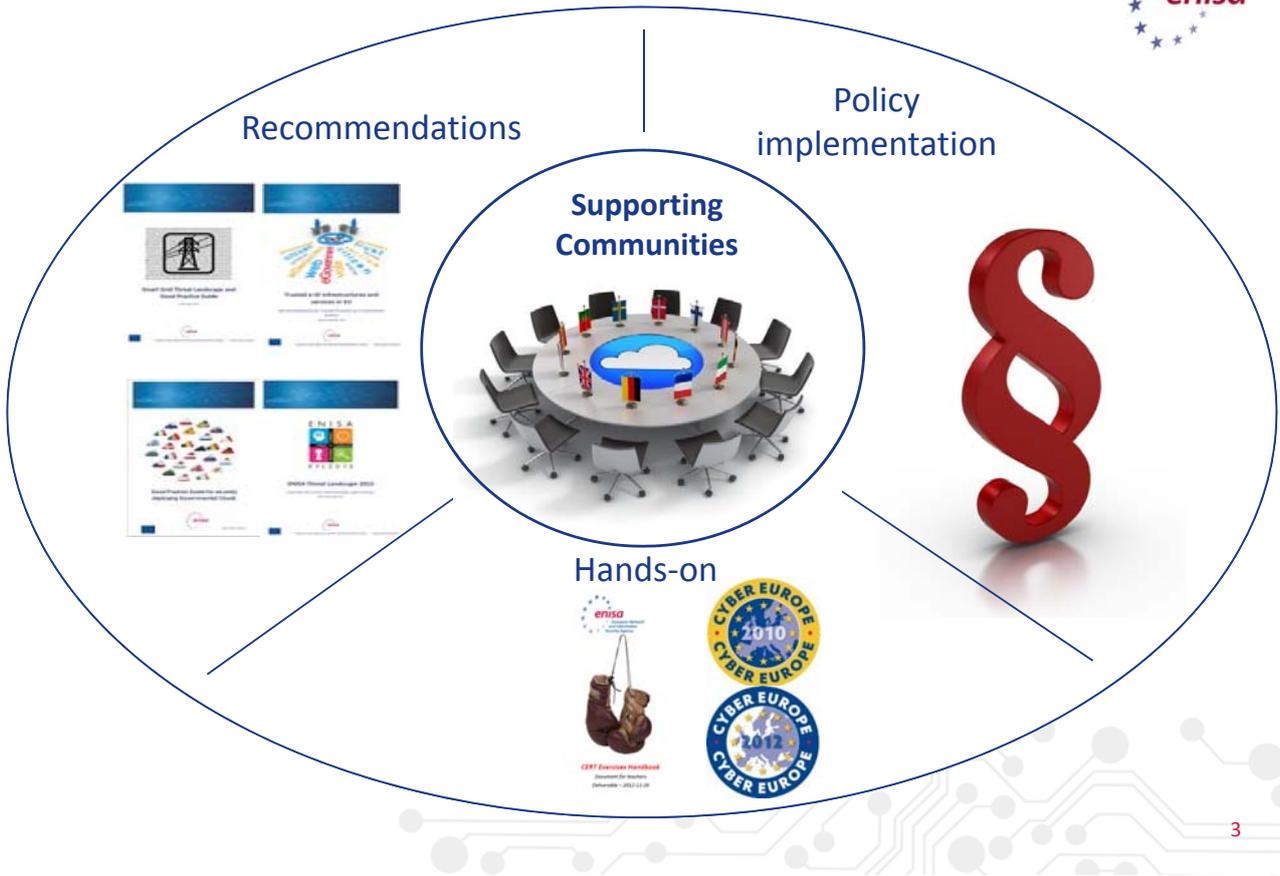
Stefan Schiffner | NIS Expert
Sommerakademie | Kiel | 31. August 2015

European Union Agency for Network and Information Security



ENISA





Welcher Service ist Vertrauenswürdig?



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?



DON'T KNOW
OR NO PREFERENCE



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?



The screenshot shows the DB Bahn website interface. At the top, there are several promotional banners: 'Online-Tickets ändern oder stornieren', 'Neue Angebote, Gutscheine und mehr', 'Städtereisen & Urlaub' (with a table of offers), 'Deutschland erleben!', and 'Buchung Ihrer Fahrradkarte'. Below these are sections for 'DB Bahn im Social Web' and 'Fahrplan & Buchung'. A red navigation bar at the bottom contains links like 'Impressum', 'AGB', 'Nutzungsbedingungen', 'Datenschutz', 'deutschebahn.com', 'Karriere', 'Kooperationen', and 'bahnhof.de'. The page number '11' is visible in the bottom right corner.

Verifikation eines Siegels



The screenshot shows a security notice on the DB Bahn website. The header includes the DB Bahn logo and navigation links. The main content area features a red banner with the text 'Ihre persönlichen Daten sind auf bahn.de sicher!' and a sub-header 'DEKRA Zertifizierung'. Below this, there is a paragraph explaining the company's commitment to data security and a list of 'Zertifikate und Grundsätze' including 'DEKRA ISO Zertifizierung', 'Unsere Datenschutzgrundsätze', and 'Kreditkartenzahlung'. The page number '12' is visible in the bottom right corner.



Verifikation eines Siegels

The image shows two screenshots from a website. The top screenshot is from the DB BAHN website, displaying a security notice titled "Ihre persönlichen Daten sind auf bahn.de sicher!". It includes sections for "Allgemeine Informationen", "DEKRA Zertifizierung", and "Zertifikate und Grundsätze". The bottom screenshot is from the DEKRA website, showing a page for "Qualitätsmanagement nach ISO 9001". It features a navigation menu, a search bar, and a main content area with a photo of a man pointing at a diagram. A red number "13" is visible in the bottom right corner of the DEKRA page.



Did you ever verify?



Definition und Beispiel-Instanz eines OSPS



Service publiziert Bewertung

- Graphische Darstellung
- Fälschungssicher
- Negative Bewertungen



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 Vertrauensmodelle, Standards
2. Standards müssen die Serviceart, Datenschutz- und Sicherheitsanforderungen, Evaluationsrichtlinien, und Häufigkeit einschließen
3. Zufallskontrollen, vorbereitende Maßnahmen für Kryptographische Lösungen



19

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



20

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
Luxembourg

Annual
Privacy
Forum

