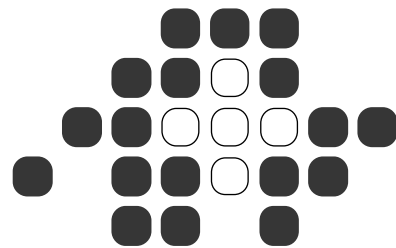




Digitale Identitäten in der öffentlichen Verwaltung

Marcel Frauenknecht



Informatikstrategieorgan Bund ISB

Unité de stratégie informatique de la ConfédérationUSIC

Organo strategia informatica della Confederazione OSIC

Organ da strategia informatica da la confederaziun OSIC



Situation in der Bundesverwaltung (BVerw)

In der BVerw werden verschiedene Identifikations- und Authentifikationsverfahren eingesetzt

Digitale Zertifikate stellen eine Möglichkeit dar

Es gibt keinen Zwang zum Einsatz von Zertifikaten bzw. Zertifikaten einer bestimmten Ausprägung

Das Interessante an digitalen Zertifikaten ist die Möglichkeit, Verbindlichkeitsdienste anzubieten



Wie will der Bund den Bürger digital identifizieren?

Antwort: Applikationsspezifisch – wenn überhaupt

Abklärungen im Rahmen des Projekts elektronische ID (eID) Karte haben gezeigt, dass Bürger vom Bund selten identifiziert und authentifiziert werden müssen (Interaktionen finden meist über die Gemeinden statt)



Welche digitalen Identitäten verwenden die Kantone?

Antwort: Verschiedene (ähnlich wie BVerw)

An der Schnittstelle zur BVerw werden in erster Linie Zertifikate des BIT eingesetzt

Klassen C und D → Firewall-Traversierung (FW-KTV)

Klasse B → Firewall-Traversierung (FW-KTV)
SSO-Portal (EJPD)



Welche Zertifikate benötigen Mitarbeiter der öffentlichen Verwaltung?

	HW/SW	Registrierung	Funktion	Bemerkungen
A	HW	persönlich	Signierung	ZertES-konform
B	HW	persönlich	alle	ehem. Klasse 3
C	SW	administrativ	alle	C-Enterprise C-TrustCenter
D	SW/HW	administrativ	Authentifizierung	ehem. Klasse 2



Weshalb kommen Zertifikate zum Einsatz?

Antwort: Für die Umsetzung von Verbindlichkeitsdiensten (im Sinne von digitalen Signaturen) ist die asymmetrische Kryptographie (und damit Zertifikate) unabdingbar

Für alle anderen Dienste (insbesondere Authentifikationsdienste) gibt es Alternativen

Man erhofft sich durch den Einsatz von Zertifikaten Synergieeffekte



Wer stellt die Zertifikate aus?

Antwort: In der BVerw gibt es einen Grundsatz-entscheid des IRB

Demnach werden alle höherwertigen Zertifikate innerhalb der BVerw von der Admin PKI des BIT ausgegeben (d.h. es gibt neben der Admin PKI in der BVerw keine andere PKI)



Welche Prozesse sind dazu erforderlich?

Antwort: Die Prozesse sind in der Certificate Policy (CP) bzw. im Certificate Practice Statement (CPS) des BIT beschrieben



Welche Rolle spielt die Smartcard in diesem Umfeld?

Antwort: Für die Zertifikatsklassen A und B ist der Einsatz von Smartcards (oder vergleichbaren Hardware-Tokens, wie z.B. USB-Tokens) zwingend erforderlich

Das BIT setzt Smartcards von Safenet (Ex-Datakey) (und in Zukunft auch Siemens) ein



Wer ist für das Management der Smartcards verantwortlich und welche Anforderungen muss diese Organisation erfüllen können?

Antwort: Die OE's sind verantwortlich

Die Anforderungen sind im Prinzip von der BVerw selbst auferlegt (ausser für Klasse A)