



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Status quo eIDAS – Deutschland im 6ten Jahr

Status quo eIDAS - Anbindung an das eIDAS Netzwerk

Die dt. Online Ausweisfunktion ist an **19 MSen** sowie an die **EU-KOM** angebunden.



12 eID Systeme müssten von dt. Diensten angebunden werden



- Die tatsächliche Nutzbarkeit von Diensten in den MSen ist stark unterschiedlich.
- In manchen MS benötigen öffentliche Dienste eine nationale Bürgerkennziffer, die z.T. aber nur durch Offline-Prozesse zu erhalten ist.

- Aktuell haben 15 MS eID-Lösungen notifiziert, weitere Länder haben Notifizierungen angekündigt
- **Bis jetzt ist kein einziger deutscher Onlinedienst funktionsfähig angebunden.**

Notwendige Optimierungen des eIDAS Frameworks

- **Vermehrung** der nutzbaren **Dienste**

- Erweiterung der Anerkennungsverpflichtung auch auf den regulierten Teil des privaten Sektors
- ...

- **Verbesserung** der Beteiligung des **privaten Sektors**

- Vereinfachung von Zugangs- und Zahlungskonditionen zur Nutzung von notifizierten eIDs
- Verkürzung, Vereinfachung und Beschleunigung des Notifizierungsprozesses
- ...

- **Vermehrung** der Zahl der MSen mit **notifizierten eIDs**

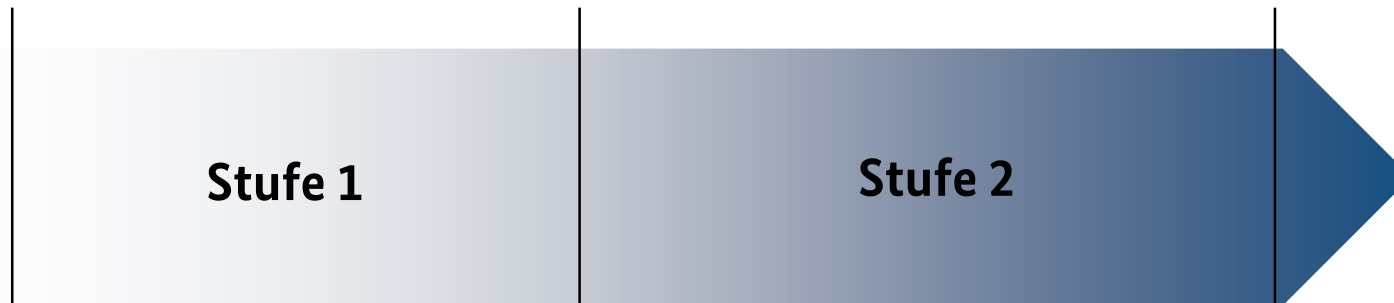
- Wiedernutzung von Teilen notifizierter eID Schemata in anderen MS oder durch private Firmen
- Reduzierung der Komplexität des Notifizierungsprozesses
- Finanzielle Unterstützung der Staaten
- ...

Optimierung des eIDAS Frameworks - Evolutionärer Ansatz

Verbesserungen wie z.B.:

-) Einführung der „Building Blocks“
-) Harmonisierung von Verordnungen
-) Beteiligung des priv. Sektors
-) Übermittlung zusätzlicher Attribute

Start



Stufe 1

Stufe 2

Ziel:

Ein europaweites, einfaches, vertrauenswürdiges und sicheres System zur Verwaltung von Identitäten im digitalen Raum.

Weiter Verbesserungen wie z.B.:

-) Notifikation SE-basierte Lösung als „Building Block“
-) Einführung eines Verwaltungssystems für zusätzliche Attribute

Vorteile von SEs als sichere Vertrauensanker in mobilen Geräten

- Nachteile bei Verwendung von reinen Softwarelösungen
 - Fehlender Schutz gegen diverse Angriffe (Kopieren,...)
 - Schwächste Lösung!



- Vorteile einer Verwendung von SEs

- Höhere Resistenz gegen Angriffe
- Zertifizierung möglich

} Z.B.: eID basierend auf OPTIMOS

- Vorteile einer Verwendung von Smartcards

- Entwicklung, Produktion und Ausgabe kontrollierbar
- Stärkste Lösung!



Rechtlicher Rahmen auf EU- und MS-Seite

- Das „**EU coordinated risk assessment of the cybersecurity of 5G networks**“ identifizierte das durch die Anzahl und Vielfalt von Nutzer Endgeräten verursachte Risiko.
- Die "Cybersecurity of 5G networks **EU Toolbox** of risk mitigating measures“ beschreibt daher zertifizierte Module (z.B. eSIM) als Risikominimierende Maßnahme.

→ Folglich:

- Die Nutzung von zertifizierten SEs/eUICCs (Kat.3) als Vertrauensanker, soll verpflichtend werden.
- Ein regulatorischer Rahmen für die Nutzung von SEs/eUICCs in einem europäischen Zertifizierungsprozesses unter dem CSA wir benötigt.
- Notifizierten eID Systemen muss ein nicht diskriminierender Zugang zu den SSs/eUICCs gestattet werden.

Optimierung des eIDAS Frameworks - “Building Blocks”

SE-basierte Lösung als wiedernutzbarer und renotifizierbarer “Building Block”:

Building Block
Authentifikation

- **Detaillierte techn. Spezifikation einer SE-Lösung** (inklusive zugehöriger CC PPs)
- Definition von **Evaluations- und/oder Auditprozedur**
- Beschreibung der **Testmethodologie und -tiefe** (z.B. CC)
- Beschreibung des **Aufsichtsregimes** (SOGIS/EU-CC/CSA)

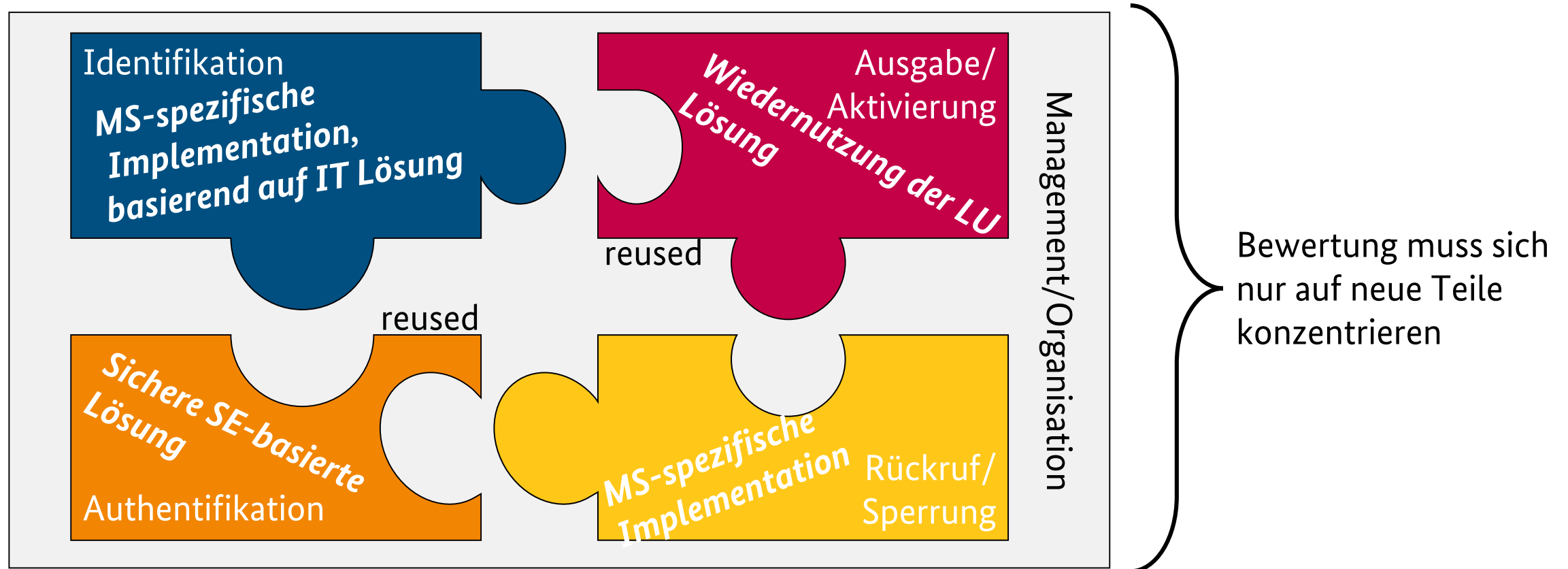
→ “Building Block” wird **einmal** im Kontext einer **Notifikation** bewertet

→ Kann **einfach** durch MSen oder IdPs **wiederverwendet** werden

→ **Renotifizierung** wird **vereinfacht**

Optimierung des eIDAS Frameworks – Die Vision

Zusammenbau der eigenen Notifikation aus Wiederbenutzern und selbst entwickelten “Building Blocks”



→ Erlaubt ein kürzeres Peer-Review und einen schnelleren Notifizierungsprozess

Optimierung des eIDAS Frameworks - Evolution vs. Revolution

Vorteile	„Building Blocks“	Qualified eID	EU-eID
Mehr grenzüberschreitend nutzbare eIDs	✓ ¹⁾	✓	✓
Mehr nutzbare Dienste	✓ ¹⁾	✓	✓
Größere Beteiligung des privaten Sektors	✓ ¹⁾	✓	✓
Nutzung des eIDAS Interoperabilitätsframeworks	✓	✗	(✓) ²⁾
Schützt getätigte Investitionen (z.B. im privaten Sektor)	✓	✗	(✓) ²⁾
Fördert aktuelle Aktivitäten und verbessert Framework	✓	✗	(✓) ²⁾
Fördert eine Harmonisierung der eID Landschaft	✓	✗	✓
Fördert eine Kooperation zwischen den MSen	✓	✗	✗
Schützt die nationale Souveränität bei eIDs	✓	✗	✗
Verbessert die Nutzung kurzfristig	✓	✗	✗

1) Z.B.: Vereinfachung des Notifizierungsprozesses, die Klärung von Zugangs-/Kostenbedingungen privater Parteien und Erweiterung der Anerkennungsverpflichtung

2) Wenn die EU-eID auf dem aktuellen eIDAS Netzwerk beruht

Auf dem Weg zu einer EU-eID

- Eine EU-eID soll:
 - die nationale Souveränität bzgl. eIDs schützen
 - auf dem aktuellen eIDAS Framework fußen
- Eine EU-eID benötigt:
 - eine Regulatorische Basis für ein verpflichtendes SE, um ein gleiches Sicherheitsniveau sicherzustellen
- Eine EU-eID darf nicht:
 - bereits notifizierte eID Schemata ersetzen
 - den aktuellen Aktivitäten im eIDAS Umfeld schaden
 - die Investitionen von privaten Firmen riskieren

Möglich unter bestehendem Framework!

(z.B. als **SE-basierter Authentisierungs-“Building Block”** mit **“EUid” als Label** für eIDs, die eIDAS-kompatible Standard-“Building Blocks” verwenden.

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Bernd Kowalski
Abteilungspräsident
Bernd.Kowalski@bsi.bund.de
Tel. +49 (0) 228 99 9582-5700
Fax +49 (0) 228 99 10 9582-5700

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Abteilung DI - Cyber-Sicherheit in der Digitalisierung und für elektronische Identitäten
Postfach 200363
53133 Bonn

www.bsi.bund.de

