Kein Ende mit „Ende zu Ende“:

Das Verschlüsselungskonzept bei De-Mail und EGVP – Unterschiede und Gemeinsamkeiten

Workshop des SIV-ERV und der EEAR

De-Mail und die Justiz Chancen für den Elektronischen Rechtsverkehr

03. Februar 2011

Vertretung des Saarlandes beim Bund, Berlin

Jürgen Ehrmann

Baden-Württemberg

JUSTIZMINISTERIUM

Baden-Württemberg

JUSTIZMINISTERIUM

PRESSESTELLE

MEDIENINFORMATION 28. Januar 2011

5. Europäischer „Tag des Datenschutzes“ am 28. Januar 2011

Goll: „Datenschutz ist Bürgerschutz vor dem Staat und durch den Staat“

Anlässlich des „Tages des Datenschutzes“, der am 28. Januar 2011 zum fünften Mal begangen wird, erklärte Baden-Württembergs Justizminister Prof. Dr. Ulrich Goll (FDP) heute in Stuttgart:

„Der ‚Tag des Datenschutzes‘ ruft allen Verantwortlichen und Betroffenen die große Bedeutung dieses Themas ins Bewusstsein. Datenschutz ist eine hochaktuelle Angelegenheit. Die rasante technische Entwicklung der vergangenen Jahre führt zu ganz neuen Herausforderungen für Bürgerinnen und Bürger und für die Politik. Denn beim Datenschutz geht es schon lange nicht mehr nur um den Schutz des Bürgers vor dem Staat. Es geht auch um den Schutz des Bürgers durch den Staat, der der Datensammelwut durch private Firmen gesetzliche Grenzen setzen muss. Datenschutz ist Bürgerschutz - vor dem Staat und durch den Staat“, betonte Goll.

Gefragt ist politische Gestaltung und nicht bloßes Dagegensein

Kein Ende mit „Ende zu Ende“

Experte: Dr. Thomas Lapp
Rechtsanwalt und Mediator
27.01.2011, 19:56 Uhr
Die Einführung der sogenannten „De-Mail“ steht unmittelbar bevor. Derzeit läuft das parlamentarische Verfahren zum De-Mail-Gesetz. Nach Inkrafttreten des Gesetzes sollen Bürger, Wirtschaft und Verwaltung ab dem Frühjahr 2011 auf einfache Weise rechtssicher, verbindlich und vertraulich elektronisch kommunizieren können. Auch der Elektronische Rechtsverkehr soll von „De-Mail“ profitieren.
Eine Expertenrunde diskutiert auf Initiative des Deutschen EDV-Gerichtstages, der NIFIS und der EEAR am 3. Februar 2011 in Berlin die rechtlichen und technischen Rahmenbedingungen sowie die Möglichkeiten, die sich für den Ausbau des Elektronischen Rechtsverkehrs aus De-Mail ergeben.
Donnerstag, 3. Februar 2011, 10-17 Uhr in der Vertretung des Saarlandes beim Bund, Berlin

ITAnwältin,28.01.2011, 09:53 Uhr
Ich halte De-Mail in der jetzigen Konzeption für den elektronischen Rechtsverkehr aus datenschutzrechtlichen Gründen für nicht praktisch nutzbar. Quasi jeder anwaltliche Schriftsatz enthält personenbezogene Daten - insb auch solche i.S.d.§ 3 Abs. 9 BDSG, also mit erhöhtem Schutzbedarf. Wenn diese an das Gericht übermittelt werden, dann ist zu gewährleisten, dass sie nicht unbefugt gelesen oder kopiert werden können. Dabei handelt es sich (zumindest nach Auffassung der Datenschutzbehörden) um eine nicht disponible gesetzliche Verpflichtung, der nur nachgekommen werden kann, wenn entweder die Dateine selbst verschlüsselt werden, oder ein „sicherer“ Kommunikationsweg (d.h. mit „Ende-zu-Ende-Verschlüsselung“ zum Einsatz kommt. Einen solchen Kommunikationsweg stellt De-Mail aber nicht dar.

V. M.30.01.2011, 11:46 Uhr
Man sollte nicht durch ständige Verweise auf datenschutzrechtliche Bedenken den technischen Fortschritt aufzuhalten versuchen!

Kein Ende mit „Ende zu Ende“

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 15.12.2005:

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen.
Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheitsstandard für eGovernment-Anwendungen zur Verfügung.
…
Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten … die getroffene Festlegung, den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen.

Um die angestrebte Ende-zu-Ende Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

Kein Ende mit „Ende zu Ende“

Bundesrat Drucksache 645/1/10 16.11.10 877. Sitzung des Bundesrates am 26. November 2010
Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften

…

4. Der Bundesrat hält es jedoch für erforderlich, dass eine Ende-zu-Ende-Verschlüsselung der Daten vorgenommen wird.

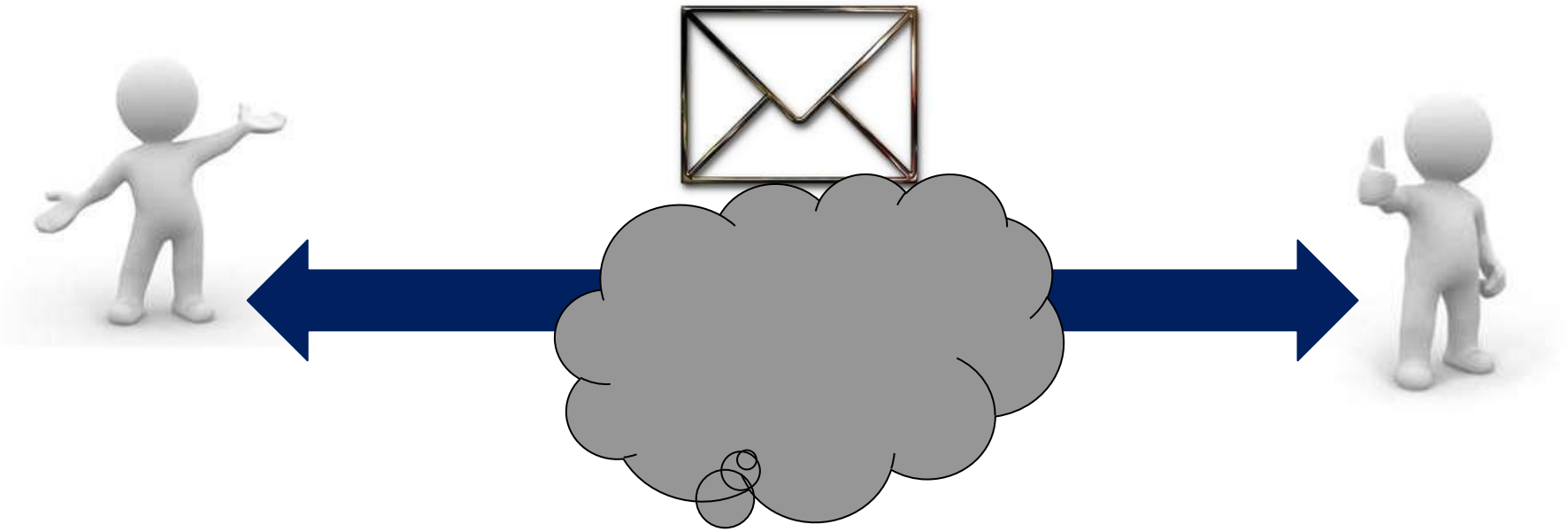
Begründung:

Der Bundesrat hält eine Ende-zu-Ende-Verschlüsselung der Daten für erforderlich. Nach dem Gesetzentwurf ist lediglich eine Verschlüsselung durch gängige Standards für sicheren Mailversand (SSL, SMTP/TLS) gewährleistet, geht aber nicht darüber hinaus. Sie wird zudem nur innerhalb des De-Mail-Netzwerkes aufrecht erhalten. Verschlüsselt wird allein der Transport, nicht aber die Nachricht selbst.
Eine Ende-zu-Ende-Verschlüsselung findet nicht statt, die Nach-richten werden zur Überprüfung von Viren und zur Prüfung, ob es sich um eine SPAM-Mail handelt kurzfristig entschlüsselt.

Während dieses Vorganges sind die Nachrichten einem erhöhten Risiko des Angriffes durch unbefugte Dritte ausgesetzt. Der Bundesrat hat daher datenschutzrechtliche Bedenken gegen die vorgesehene Verschlüsselung und fordert die Bundesregierung auf, eine Ende-zu-Ende-Verschlüsselung vorzusehen.

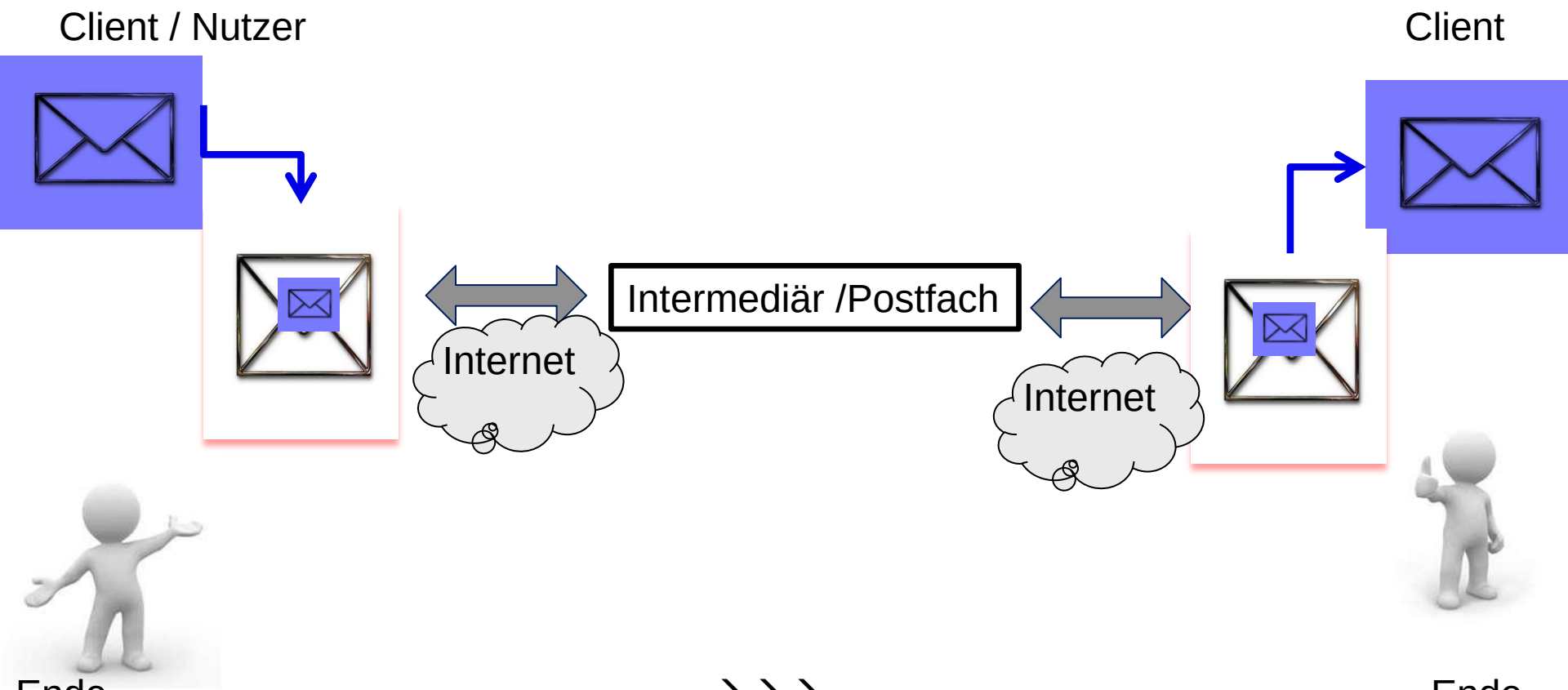
…

Kein Ende mit „Ende zu Ende“

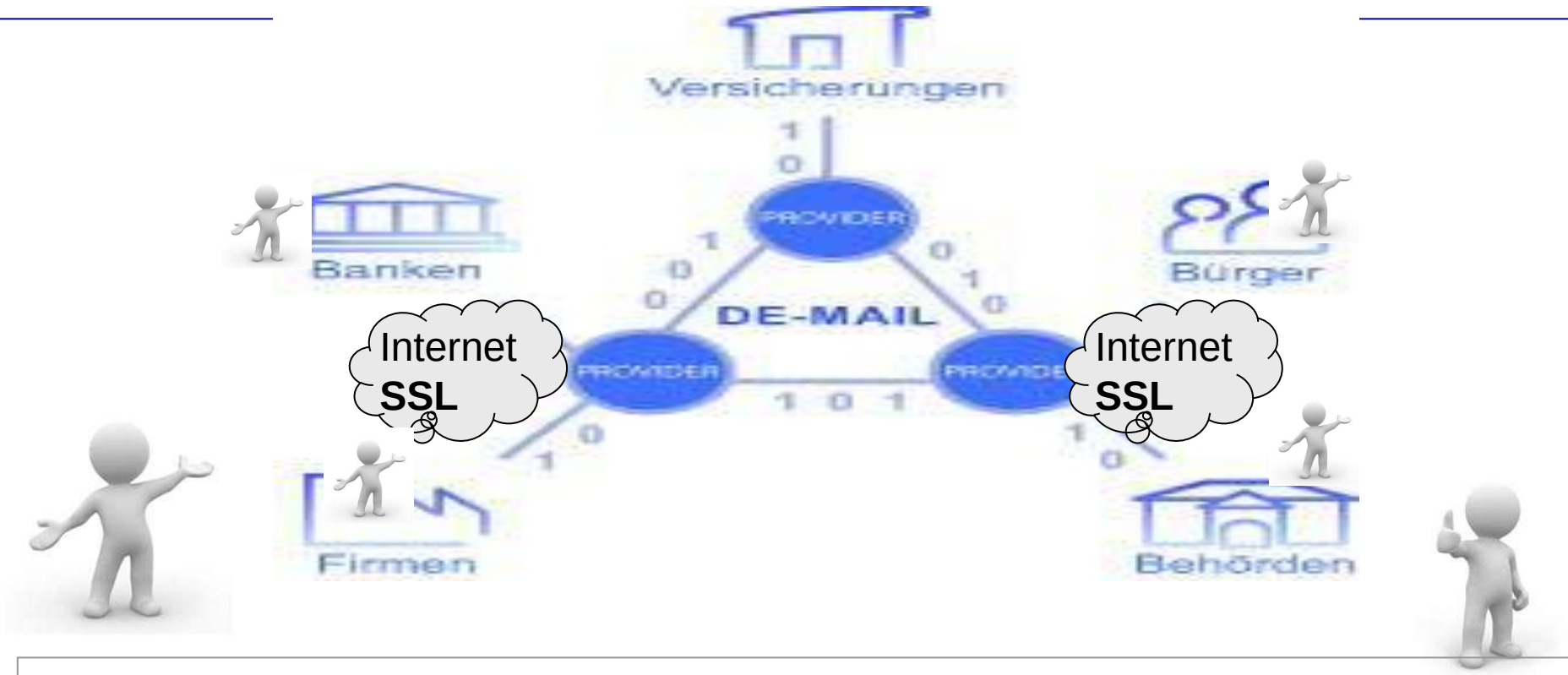


Ende zu Ende ein ***Kampfbegriff?***

Elektronisches Gerichts- und Verwaltungspostfach EGVP (OSCI 1.2 bzw. OSCI 2.0)



De - Mail



Ende →→→	Umschlüsseln/Virenscanner →→→	Ende
Nutzer → → →	De-Mail Provider1 ---- De-Mail Provider2 →→→	Nutzer

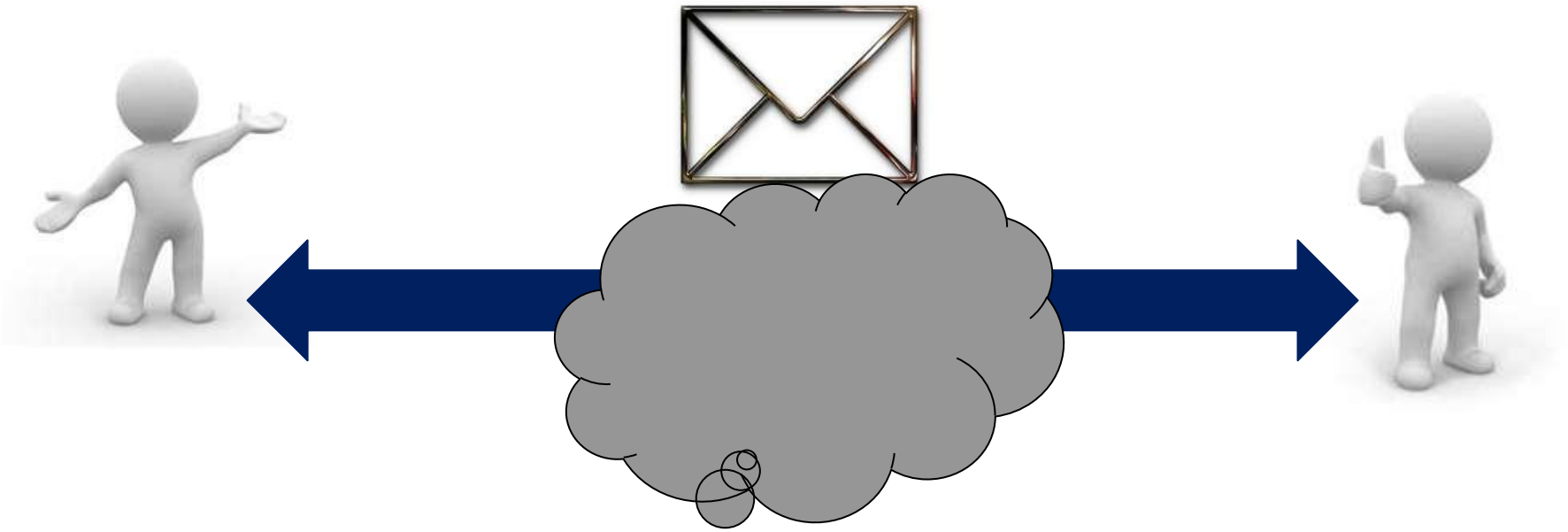
Option: Verschlüsselung mit Verschlüsselungszertifikat aus Verzeichnis

De - Mail

NEIN!

- Die Vertraulichkeit von sensiblen Daten wird auf ihrem Weg vom Sender zum Empfänger durch Verschlüsselung der De-Mail-Nachrichten innerhalb des De-Mail-Verbundes stets gewährleistet. Das bewirkt der Einsatz von Transport- und nachrichtenbezogenen Verschlüsselungsfunktionen.
- In Fällen, in denen Sender und Empfänger die übermittelten Daten zusätzlich mit ihren eigenen Ver- bzw. Entschlüsselungsschlüsseln ver- bzw. entschlüsseln möchten, ist eine Integration von entsprechenden Lösungen für die zusätzliche Ende-zu-Ende-Verschlüsselung mit De-Mail möglich.
- Nutzer, die zusätzlich Ende-zu-Ende verschlüsseln wollen, werden nach den De-Mail-Konzepten hierbei unterstützt. Nach den Technischen Richtlinien von De-Mail, die Grundlage für die Zulassung der künftigen De-Mail-Provider sind, sind die De-Mail-Provider verpflichtet, auf Wunsch der Nutzer deren eigene Verschlüsselungszertifikate im öffentlichen Verzeichnisdienst zu veröffentlichen. Hierdurch wird ein wesentlicher „Hemmschuh“ für die Verbreitung der Ende-zu-Ende-Verschlüsselung („Wo finde ich einen gültigen Verschlüsselungsschlüssel des Empfängers?“) durch De-Mail beseitigt. Die Verbreitung von Lösungen für die Ende-zu-Ende-Verschlüsselung kann so durch De-Mail maßgeblich unterstützt werden.

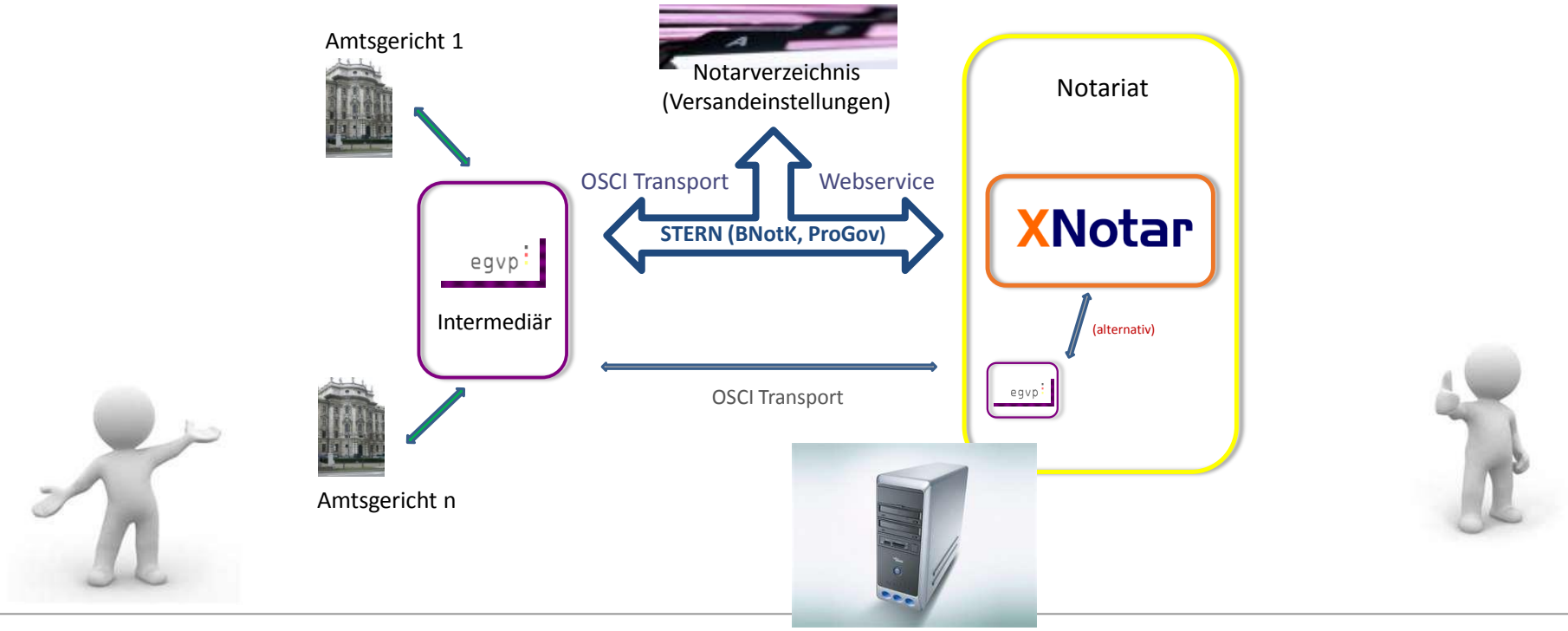
Kein Ende mit „Ende zu Ende“
Lücke im System?



Fazit: ➔ Sicherheitslücke bei De-Mail?

Kein Ende mit „Ende zu Ende“ -- Lücke im System?

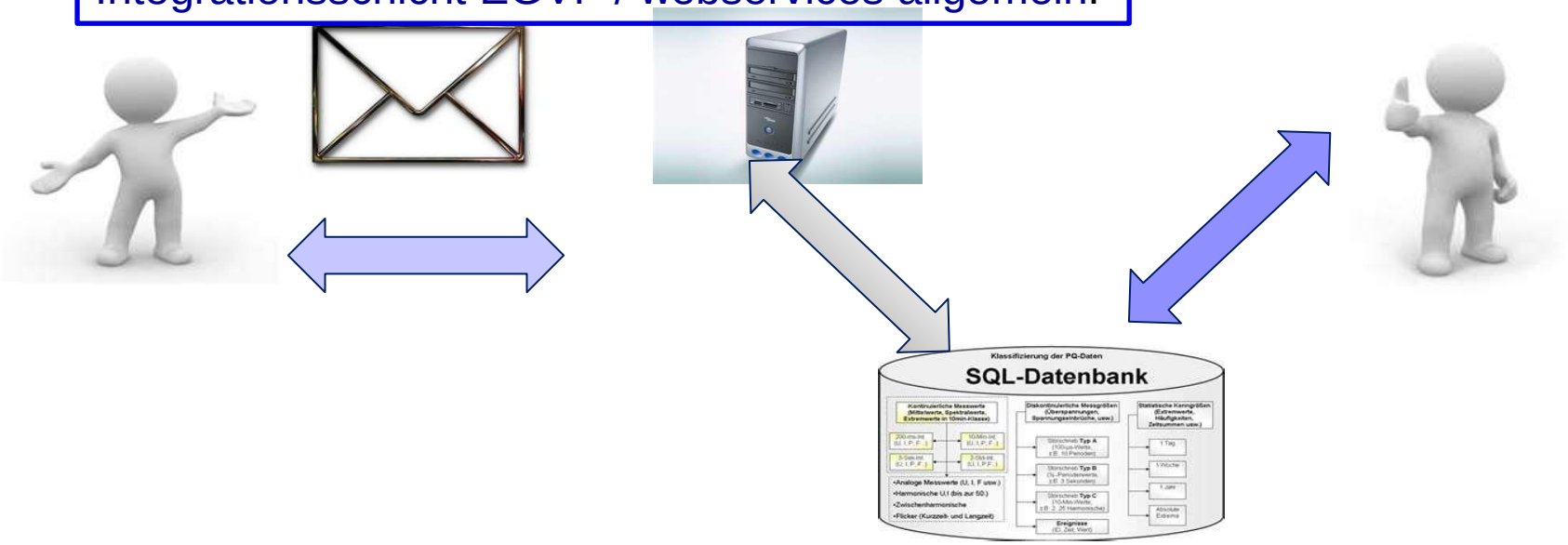
Nachrichtenverkehr der Notare über das EGVP - Kommunikationsplattform der BNotK:



Ende	→→→	Ende → → webservice
Person	→→→	FA

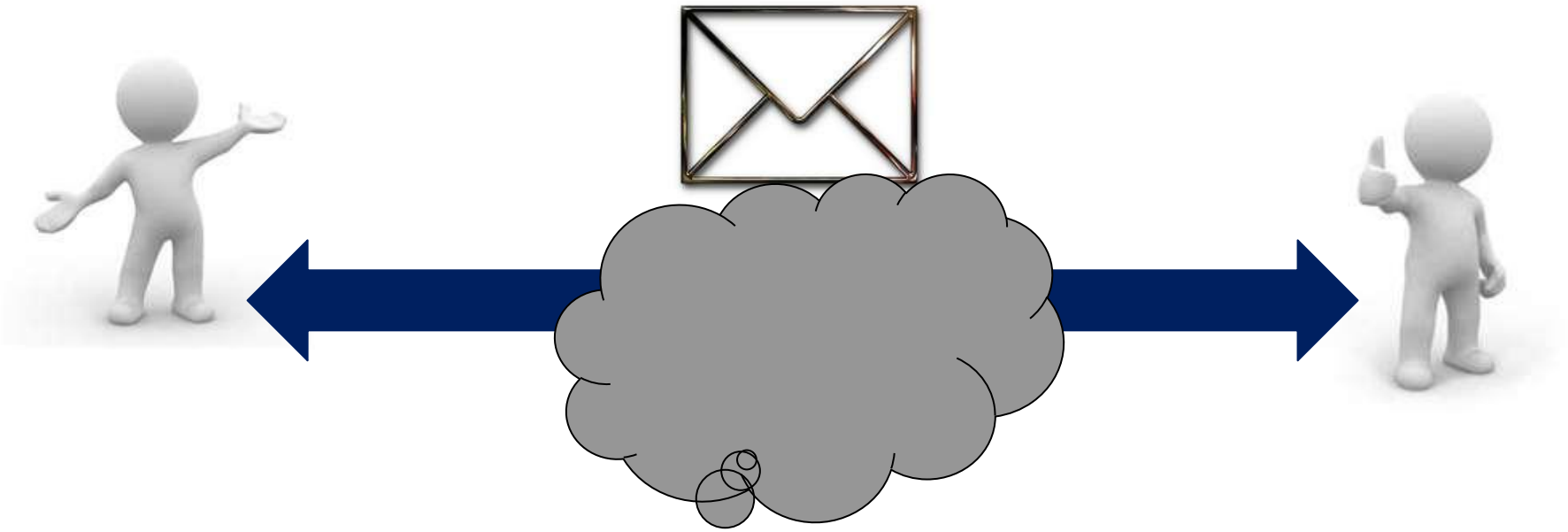
Kein Ende mit „Ende zu Ende“ -- Lücke im System?

Integrationsschicht EGVP / webservices allgemein:



Landesverwaltungsnetz BW: sichere abgeschottete Infrastruktur

Kein Ende mit „Ende zu Ende“
Lücke im System?



Fazit: ➔ Sicherheitslücke bei De-Mail? ➔**???**

➔EGVP ist das Rund-um-Sorglos-Profipaket
➔De-Mail ist E-Mail mit Zusatzfunktionen

Kein Ende mit „Ende zu Ende“
Der Vergleich

EGVP (OSCI 1.2 bzw. OSCI 2.0):

automatische Transportverschlüsselung, Ende zu Ende

Intermediär mit

- → Dokumentation Übergabe
- → Dokumentation Bereitstellung
- → Dokumentation Abholung

Adressbuch mit verschiedenen Sichtbarkeiten

- → Institutionen
- → Anwender

Anbindung an Standard eID-System S.A.F.E. mit den Identitäten aus vielen Anwendungsbereichen Justiz und Verwaltung (EU-DLR, BNotK)

professionelle „Rund-um-Sorglos“ Lösung

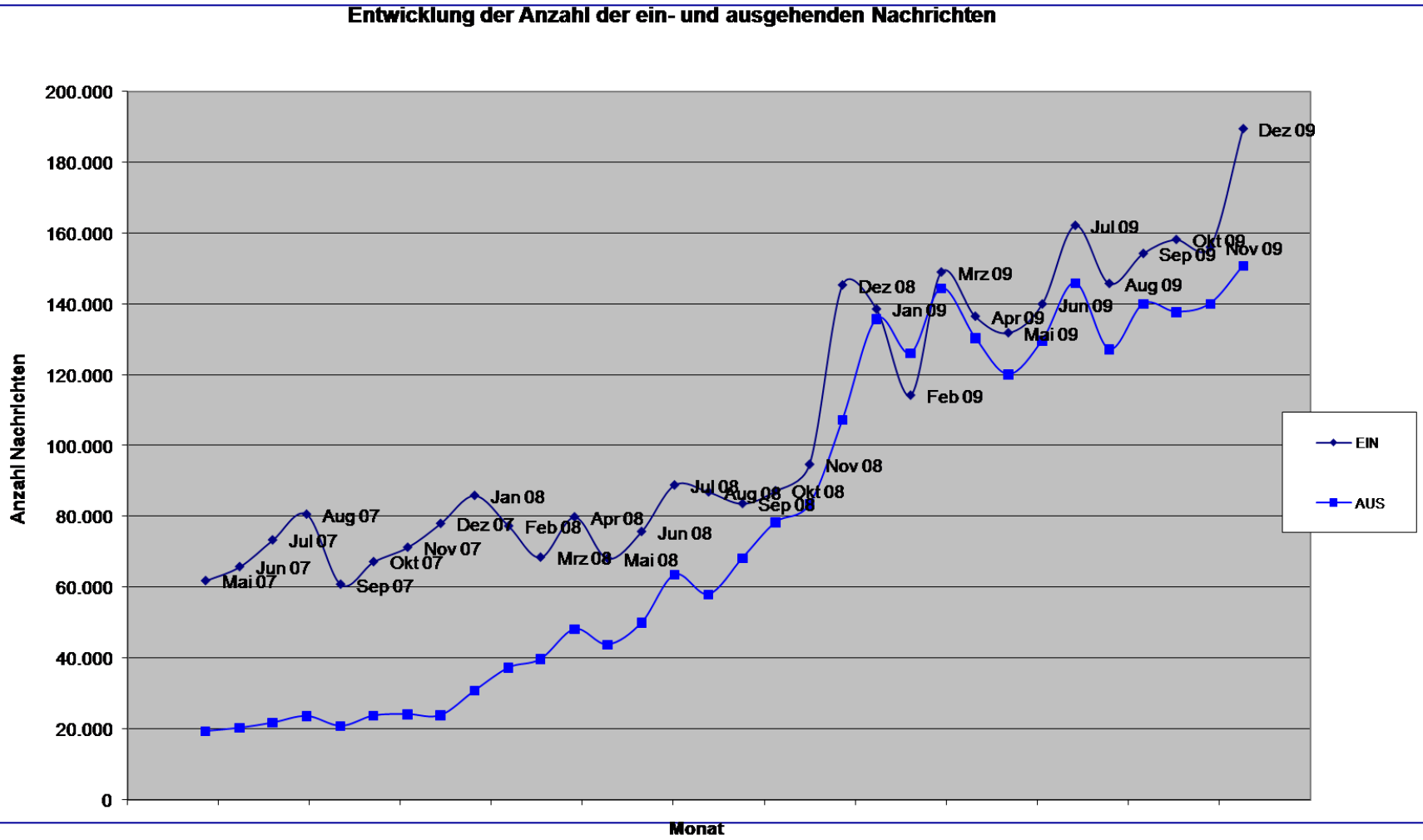
De-Mail

Einfach wie E-Mail

Ende zu Ende taugt wenig zur Unterscheidung!

?

Kein Ende mit „Ende zu Ende“
Der Vergleich



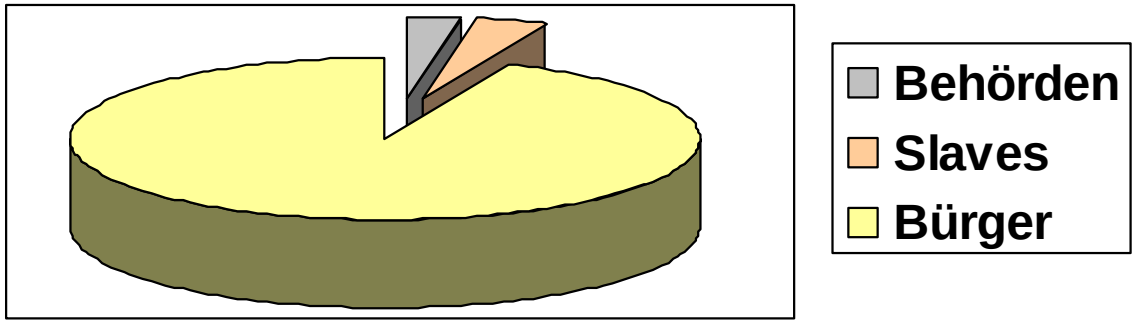
Baden-Württemberg
JUSTIZMINISTERIUM

Kein Ende mit „Ende zu Ende“
Der Vergleich

- Postfachbestand

  auf dem Registrierungsserver (Stand 09/2010)

  - Behörden 1.174
  - Slaves 1.506
  - Bürger 39.289



Kein Ende mit „Ende zu Ende“
Der Vergleich

EGVP (OSCI 1.2 bzw. OSCI 2.0):

automatische Transportverschlüsselung, Ende zu Ende

Intermediär mit

- → Dokumentation Übergabe
- → Dokumentation Bereitstellung
- → Dokumentation Abholung

Adressbuch mit verschiedenen Sichtbarkeiten

- → Institutionen
- → Anwender

Anbindung an Standard eID-System S.A.F.E. mit den Identitäten aus vielen Anwendungsbereichen Justiz und Verwaltung (EU-DLR, BNotK)

professionelle „Rund-um-Sorglos“ Lösung

De-Mail

Einfach wie E-Mail

Massive Unterstützung

Portallösung SSL-gesichert

Unterstützung Ende zu Ende in Verantwortung des Anwenders

Zertifikatsverzeichnis

?

Entwicklungspotential

Kein Ende mit „Ende zu Ende“
Der Vergleich -- Was tun?

Zu Buchstabe b:

Bei fehlender Kompatibilität des De-Mail-Verfahrens mit dem EGVP ist zu befürchten, dass mit De-Mail eine zusätzliche Kommunikationsstruktur eröffnet wird, die mit hohem Aufwand in die gerichtlichen Geschäftsabläufe integriert und überwacht werden muss. Technisch erscheint eine Anbindung von De-Mail an das EGVP möglich; hierüber gibt es bereits Gespräche zwischen Vertretern der AG IT-Standards der Bund-Länder-Kommission für Datenverarbeitung und Rationalisierung in der Justiz und des De-Mail-Projekts. Das hohe IT-Sicherheitsniveau der Kommunikation über EGVP sollte dabei aber beibehalten werden.

Die **88. BLK (November 2010, Genf)**
beauftragt die BLK-AG „IT-Standards in der Justiz“ im Zusammenhang mit S.A.F.E. und dem EGVP,
...
→ den **Einstieg in den Pilotversuch mit DE-Mail in Abstimmung mit dem BMI** weiter voranzutreiben und dabei insbesondere die **Umsetzung des OSCI-DE-Mail-Gateways** auf der Basis des „Konzepts für die Integration von De-Mail und OSCI-basiertem elektronischen Rechtsverkehr“ des BSI zu prüfen und fortzuentwickeln.
Die BLK ist sich gleichzeitig darüber einig, dass weiterhin geprüft werden soll, ob und in welchen inhaltlichen Bereichen zum Beispiel DE-Mail auch ohne OSCI-Einbindung für die Kommunikation im Justizbereich eingesetzt werden kann.

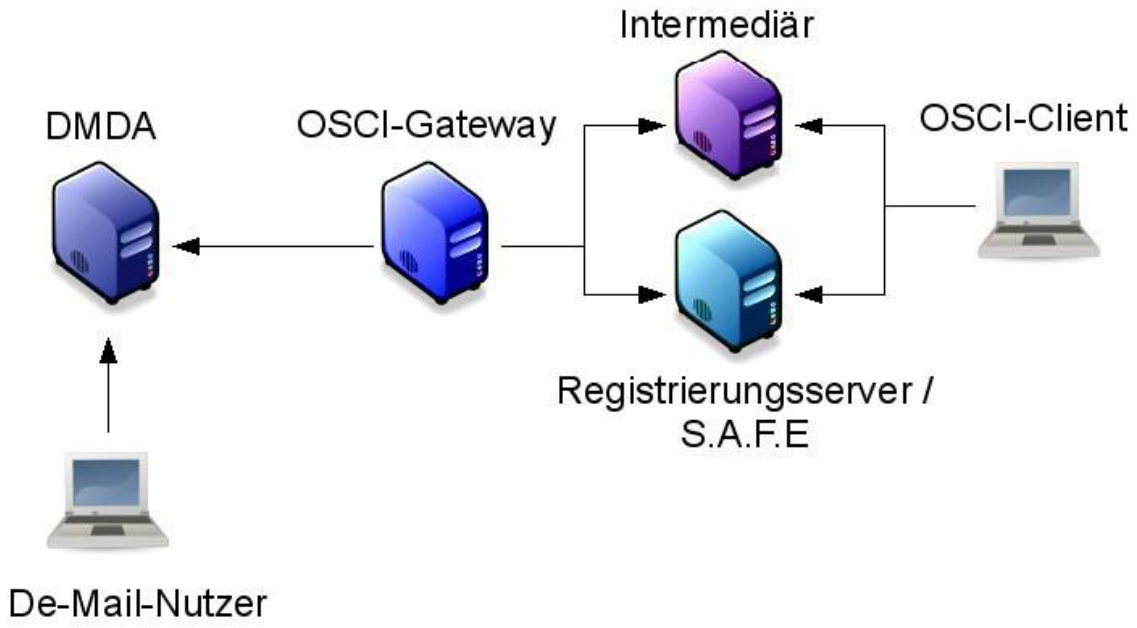
Kein Ende mit „Ende zu Ende“
Der Vergleich -- Was tun?

Pilotversuch bei einem Landgericht in Baden-Württemberg

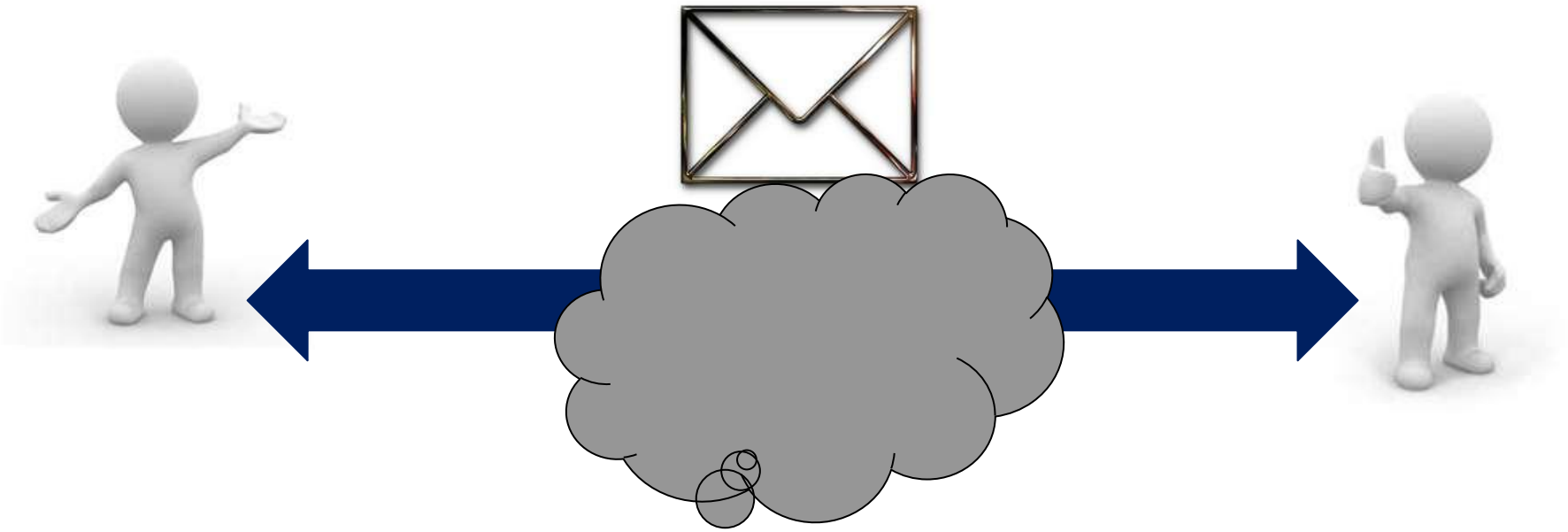
Bundesamt für Sicherheit in der Informationstechnik

Konzept für die Integration von De-Mail und OSCI-basiertem elektronischen Rechtsverkehr

(Entwurf zur Abstimmung)



Kein Ende mit „Ende zu Ende“ → Vielleicht doch..



Fazit: → Der ERV kann von zwei Wegen nur profitieren!

Besonders wenn diese verbunden werden können!

Vielen Dank für Ihr Interesse!

www.justiz.de

www.egvp.de

Jürgen Ehrmann
ehrmann@jum.bwl.de