T.I.S.P.
TeleTrusT Information Security Professional

TeleTrusT
Pioneers in IT security.

T.I.S.P. Community Meeting 2011

ISO 27001 Zertifizierung auf der Basis IT-Grundschutz

Uwe Holle
Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Ziel des Vortrages

**Ziel des Vortrages ist es,
Erfahrungen darzustellen,
auf dem Weg zu einer**

ISO 27001 Zertifizierung auf der Basis IT-Grundschutz

im Bereich der EU-Zahlstelle Niedersachsen/Bremen

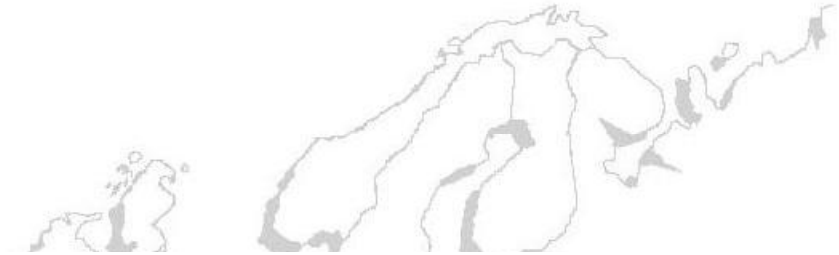
Die BSI-Standards und die IT-Grundschutz Kataloge sind auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu finden.

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

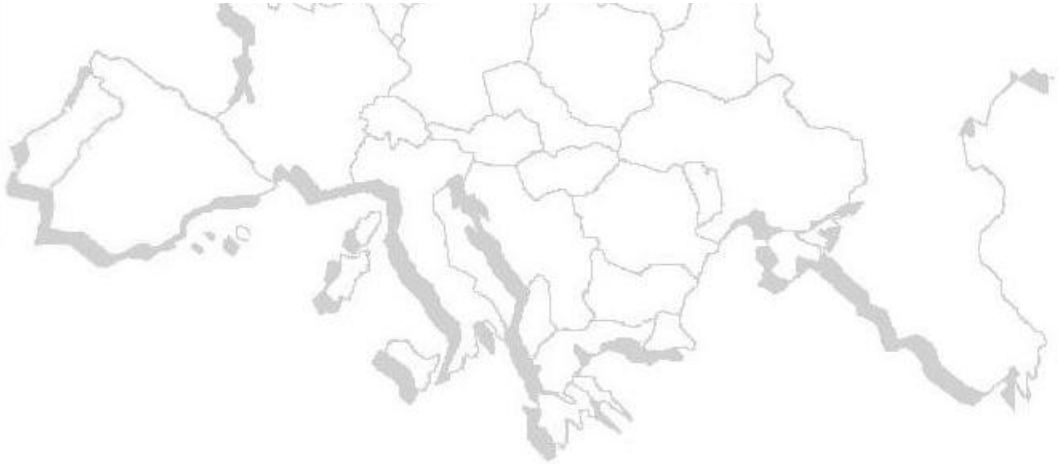
Referat 301.2
EU - Zahlstelle

Grundfragen

1.) Warum ein Zertifikat ?



2.) Was ist eine EU-Zahlstelle ?



Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Vorstellung der EU-Zahlstelle Niedersachsen/Bremen

Aufgaben einer EU-Zahlstelle

Europäischer Garantiefonds für die Landwirtschaft (EGFL)

Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER)

In Niedersachsen:
ca. 80 verschiedene Fördermaßnahmen mit einem finanziellen Volumen von jährlich ca.

1,2 Milliarden Euro

Einrichtung der EU-Zahlstelle Niedersachsen/Bremen für die Abwicklung der Fördermaßnahmen des EGFL und ELER erfolgte im

**Niedersächsischen Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung**

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Vorstellung der EU-Zahlstelle Niedersachsen/Bremen

Gesetzliche Grundlage

Verordnung (EG) Nr. 885/2006

u.a. Zulassungskriterien einer EU-Zahlstelle (Anhang I)

Punkt 3. Information und Kommunikation

B) Sicherheit der Informationssysteme

Die Zahlstelle wählt einen dieser internationalen Standards als Basis für die Sicherheit der Informationssysteme aus.

- **ISO Standard**
- **IT-Grundschutz**
- **COBIT**

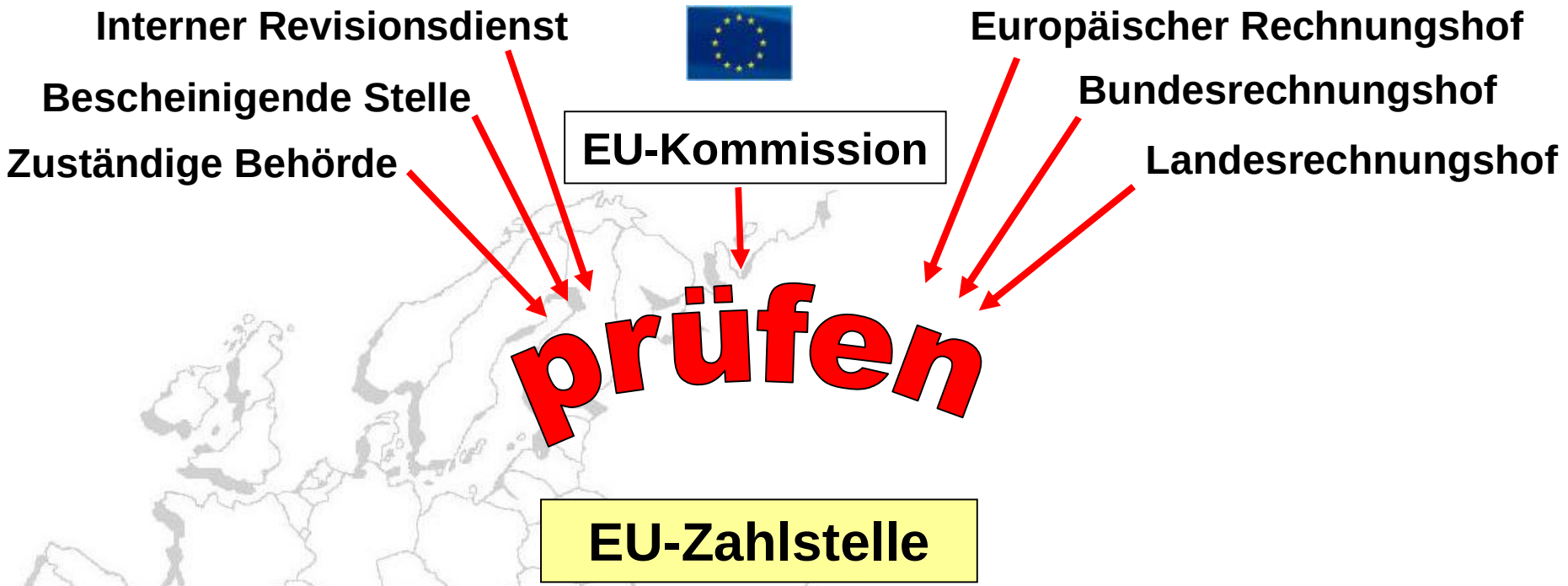
<u>Beschluss der Agrarministerkonferenz:</u> Einheitliche Anwendung des IT-Grundschutzes für die EU-Zahlstellen der Bundesrepublik Deutschland.

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Vorstellung der EU-Zahlstelle Niedersachsen/Bremen

Prüfdienste



Um den Prüfaufwand und die Prüftätigkeiten möglichst gering zu halten:

ISO 27001 Zertifizierung auf der Basis IT-Grundschutz

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Informationsverbund

Aufbau der EU-Zahlstelle

Niedersächsischen Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Leitung der EU-Zahlstelle

Auszahlung und Verbuchung

Verschiedene Fachreferate

Niedersächsischen Ministerium
für Umwelt und Klimaschutz

Verschiedene Fachreferate

Bewilligungsstellen

Landwirtschaftskammer Niedersachsen

Ämter für Landentwicklung

Niedersächsische Landesbetrieb für Wasser-
wirtschaft, Küsten- und Naturschutz

IT-Betrieb

Servicezentrum Landentwicklung und Agrarförderung

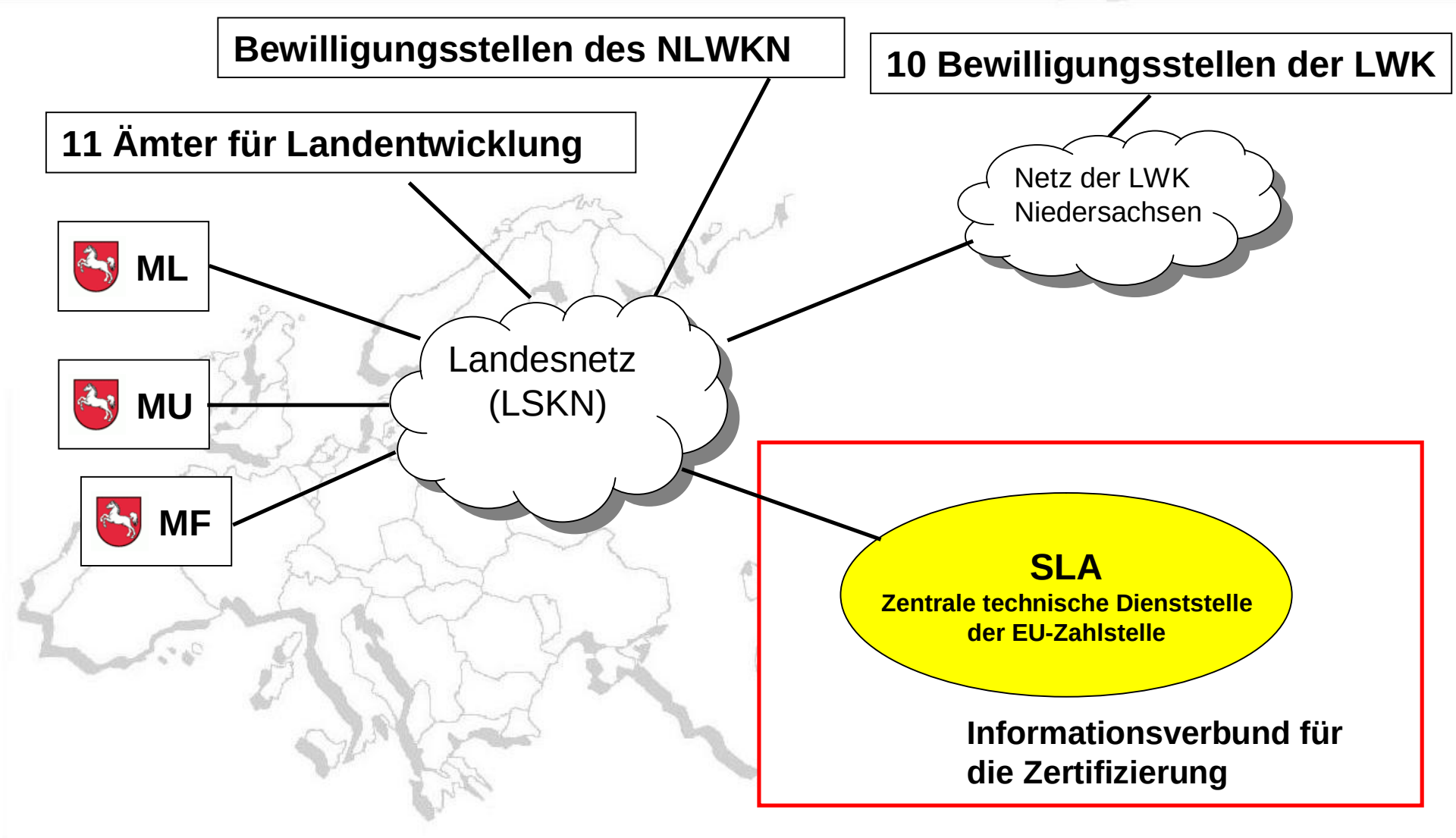
Landesbetrieb für Statistik und Kommunikationstechnologie Niedersachsen

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Informationsverbund

Technischer Aufbau der EU-Zahlstelle



Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Informationsverbund

Weitere Probleme bei der Abgrenzung

Landesnetz – Betreiber LSKN — **Technische Lösung**

Lösung Firewall

E-Mail Server **Zentral beim LSKN angesiedelt** — **Definition**

Unterstützend eingesetzt – kein Hauptgeschäftsprozess

Active Directory **Gemeinsame Domäne mit der Vermessungs- und Katasterverwaltung (LGLN)**

Formelle Regelungen - Richtlinien **Organisatorische Regelung**

Diese Ergebnisse fließen in die Leitlinie zur Informationssicherheit ein !

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Leitlinie zur Informationssicherheit

Zweck

Beschreibt die Sicherheitsziele sowie die verfolgte Sicherheitsstrategie

Inhalt

- Aufbau eines Informationssicherheitsmanagementsystems nach der Methode des IT-Grundschutzes vom BSI
- Festlegung des Geltungsbereiches – Definition des Informationsverbundes
- Verantwortung der Behörden- bzw. Unternehmensleitung für die Informations-sicherheit.
- Aufbau der Sicherheitsorganisation

  Rollenbeschreibung: z.B. IT-Sicherheitsbeauftragter,
  Bausteinverantwortlicher

  Zusammensetzung des Sicherheitsmanagementteams

Durch die Leitung in Kraft gesetzt und den Mitarbeitern bekannt gegeben !

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Jetzt geht es richtig los !

2006

Ziel: Erreichen des Auditortestates der Einstiegsstufe (alle A-Maßnahmen)

- Bundesweite öffentliche Ausschreibung

Beratung und Prüfung

Ziel erreicht: **Auditor Testat – Einstieg 0004-2006**

Gültigkeit: 30.11.2008

2007

Die Fachlichkeit muss jetzt wieder im Vordergrund stehen !

2008

Prozess der Informationssicherheit hat sich nicht etabliert und wurde von der Leitungsebene nicht entsprechend gewichtet!

Ergebnis: **Nächste Stufe wurde nicht erreicht !**
Kein Auditor-Testat oder Zertifikat liegt mehr vor!

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Und nun?

Prüfdienste bemängeln den Stand der Informationssicherheit und führen eigene Prüfungen durch.

Leitung der EU-Zahlstelle wurde aktiv.

- **Austausch des IT-Sicherheitsbeauftragten im Informationsverbund und des beratenden Auditors.**
- **Bestandsaufnahme durch den neuen Berater**
- **Aufbau des Informationssicherheitsmanagementsystems im Rahmen eines Projektes (Zieltermin: Zertifizierungsaudit muss im September 2010 durchgeführt sein.)**

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

2. Versuch

Basisinformationen lagen auf Grund der Tätigkeiten für das Auditor – Testat vor.

- **Kritischen Punkte der Infrastruktur wurden angefasst.**
  - **Brandschutz von Patchfeldern (M1.62)**
  - **Klimatisierung Rechenzentrum**
  - **Verkabelung**
  - **Brandschutzkonzept**
- **Bearbeitung der Bausteine.**
  - **Bisherige Praktiken mit den Bausteinverantwortlichen aufgenommen.**
  - **Anpassung der bisherigen Abläufe an die Anforderungen des IT-Grundschutzes.**
  - **Erstellung von Dokumentationen der Abläufe und Regelungen (z.B. Richtlinien).**

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

2. Versuch

2009 **Umbaumaßnahmen im Gebäude**

Nach der Aufnahme der Prozesse - Standardisierung

Druck auf die Leitungsebene des Informationsverbundes wurde von der EU-Zahlstelle durch die Einschaltung des Staatssekretärs erhöht.

Monatliche Berichte zum aktuellen Stand an den Staatssekretär.

2010 **Kontinuierlicher Aufbau des Informationssicherheitsmanagements**

- **Sicherheitsmanagementteam**
- **Sensibilisierungsmaßnahmen für die Mitarbeiter.**

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

2. Versuch

2010

06.Juni – Zertifizierungsantrag beim BSI gestellt

**09.Juli – Rückmeldung durch das BSI,
mit Vergabe der Zertifizierungskennung**

**04.August – Lieferung der Referenzdokumente
Beginn der Auditierung**

13.-25.August – Audit vor Ort

24.September – Abschluss der Auditierung

25.Oktober – Vorlage endgültiger Auditbericht

**17.November – Ausstellungsdatum des
ISO 27001 Zertifikates auf der Basis IT-Grundschutz**

2011

August/September – Durchführung des Überwachungsaudits

**24.Oktober – Bescheid vom BSI über den positiven Abschluss des
1. Überwachungsaudits.**

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Dank

Herrn Reto Lorenz

Tele-Consulting
security | networking | training gmbh
akkreditiert durch das BSI für Prüfungen im Bereich IT-Sicherheit

Praxisorientierte Umsetzung des IT-Grundschutzes

Positiver Umgang mit der Leitungsebene, den Bausteinverantwortlichen und den Mitarbeitern.

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Fazit

- **Leitungsebene muss absolut hinter dem Ziel stehen und nicht andere Aufgaben so priorisieren, dass die Informationssicherheit völlig nachrangig behandelt wird.**
- **geeignete Beratung ist notwendig.**
- **Klare Abgrenzung des Informationsverbundes.**
- **Viele „Aufräumarbeiten“ sind zu erledigen.**

  Beispiele: Brandschutzgutachten, Prozessbeschreibungen usw.
- **Mitarbeiter sind in die Prozesse einzubinden und bezüglich der Informationssicherheit zu sensibilisieren.**

<u>Auswirkungen</u>

- **Prozesse laufen effektiver, weil standardisiert, ab.**
- **Umgang mit Sicherheitsvorfällen ist professioneller geworden (Beispiel Stromausfall in Hannover).**

Niedersächsisches Ministerium
für Ernährung, Landwirtschaft,
Verbraucherschutz und Landesentwicklung

Referat 301.2
EU - Zahlstelle

Fragen

Vielen Dank für Ihre Aufmerksamkeit