
Legal Framework of E-Government

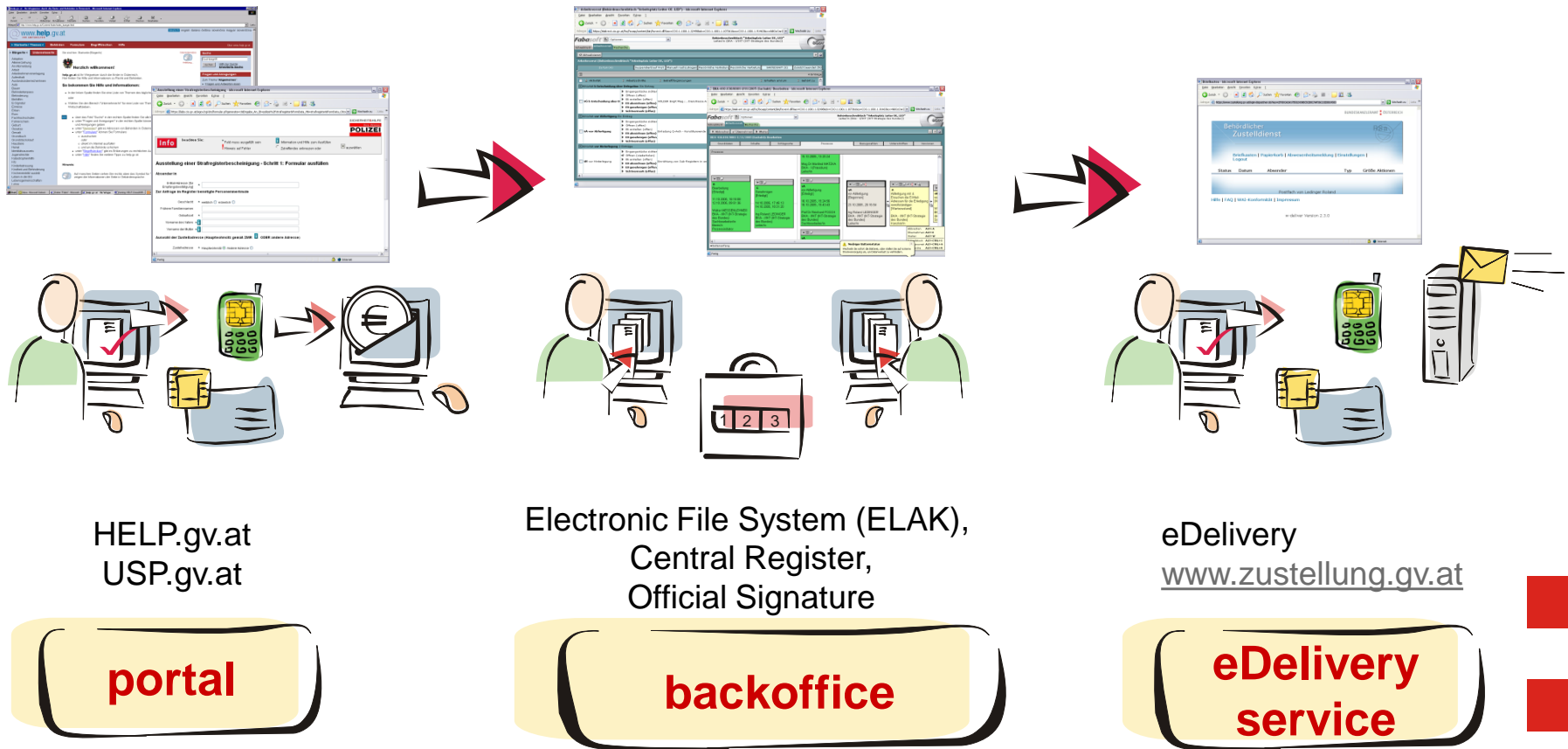


12.02.2019

Mag. Gregor Schmied
Bundesministerium für Digitalisierung und
Wirtschaftsstandort
gregor.schmied@bmdw.gv.at



Typical E-Government-Process: Goal: seamless procedures



Legal bases

Legal Bases

**E-Government
Act**

**General Admin.
Procedure Act
1991**

**Electronic
Signature and
Trust Services
Act**

**Delivery
Act**

**GDPR &
Data Protection
Act**

**Register of
Residents Act**

**Fed. Law on
Associations
2002**

Fee Act 1957

**Register of
Buildings and
Homes Act**

eID and eSignature

eIDAS Regulation and Signature and Trust Services Act

eIDAS-Regulation



- Aim:
 - To strengthen EU Single Market by boosting TRUST and CONVENIENCE in secure and seamless cross-border and cross-sector electronic transactions
 - To stimulate new business opportunities



- Background:
 - Digital Agenda
 - E-Government Action Plan 2011-2015
 - Single Market Act
 - Political Pressure by Council and European Council

eSignature – overview and legal frame

- EU Signature Directive (1999/93)
 - was replaced by EU Regulation (2014/940) on electronic identification and trust services for electronic transactions in the internal market (**eIDAS-Regulation**) by 1st July 2016
- AT Signature Act (SigG)
 - was replaced by Signatur and Trust Services Act - **SVG** (BGBl. I Nr. 50/2016)
- Signature Ordinance (SigV)
 - was replaced by Signatur and Trust Services Ordinance - **SVV** (BGBl. II Nr. 208/2016)

eSignature – overview and legal frame

- Regulation (2014/940) on electronic identification and trust services for electronic transactions in the internal market (“eIDAS Regulation“)
 - Includes eID and eSignature topic
 - directly applicable in the Member States!
 - Applicable for Trust Services since 1st July 2016
- New Signature and Trust Services Act in AT complementing the EU Regulation
 - covers procedures/ supervision of trust services (e.g. Trust Service Providers) etc.
- E-Government Act
 - was amended for further eID-details in line with eIDAS

eID (1/2)

- The Regulation does **not** require / address / contain:
 - Member States **to have** an eID scheme
 - Member States **to notify** their eID scheme(s)
 - «**Notified**» eIDs are **not** necessarily **ID cards**
 - "EU database" **of any kind**
 - "EU eID"

eID 2/2

- Voluntary notification of eID means in accordance with the **implementing acts**
- Criteria are:
 - Identity proofing at issuing side
 - Issuing process
 - Authentication mechanism
 - Issuing party
 - Technical and security specification of eID means
- Mutual recognition of notified eIDs of other MS for Assurance Level „substantial“ or „high“
- Voluntary recognition of level „low“
- For private sector voluntarily and under the conditions of the issuer

Minimum Data Set eID for a natural person

mandatory attributes:

- (a) current family name(s);
- (b) current first name(s);
- (c) date of birth;
- (d) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.

additional attributes:

- (a) first name(s) and family name(s) at birth;
- (b) place of birth;
- (c) current address
- (d) gender

Minimum Data Set eID for a legal person

mandatory attributes:

- (a) current legal name;
- (b) a unique identifier constructed by the sending Member State in accordance with the technical specifications for the purposes of cross-border identification and which is as persistent as possible in time.

additional attributes:

- (a) current address;
- (b) VAT registration number;
- (c) tax reference number;
- (d) the identifier related to Article 3(1) of Directive 2009/101/EC of the European Parliament and of the Council (1);
- (e) Legal Entity Identifier (LEI) referred to in Commission Implementing Regulation (EU) No 1247/2012 (2);
- (f) Economic Operator Registration and Identification (EORI) referred to in Commission Implementing Regulation (EU) No 1352/2013 (3);
- (g) excise number provided in Article 2(12) of Council Regulation (EC) No 389/2012

Trust service providers (TSP)

- non-qualified and qualified TSP (Art. 20 eIDAS)
- Prior authorization for qual. TSPs:
need conformity assessment report by a conformity assessment body
(Art. 21)
- Supervision on qual. TSP (Art. 17)
in Austria: Telekom-Control-Kommission / RTR (§ 12 SVG)
- reactive (ex post) measures for non-qual. TSP
(„light touch approach“)
- Trust lists of qual. TSPs and qual. TS have to be published
(Art. 22)

Requirements for qualified TSP (Art. 24 (2))

- **Staff** (expertise, reliability, experience, and qualifications + appropriate training regarding security and personal data protection rules)
- Sufficient **financial resources** and/or obtain appropriate liability insurance
- Use **trustworthy systems** and products that are protected against modification
- Have an up-to-date **termination plan** to ensure continuity of service
- Ensure lawful processing of **personal data**

Trust services – Electronic Signature

- natural person
- electronic Signatures must be admitted as evidence = „Principle of non-discrimination“
- Legal value: Qualified Signature has the equivalent legal effect of a handwritten signature
- qualified electronic signature based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic signature in all other Member States
- Art. 3 Z 12 and Art. 25 eIDAS-VO
- Innovative solutions are covered (server/ remote signing; Hardware Security Modules – HSM etc.)

Trust services – Electronic Seal



- legal person (broad notion!)
- like a digital stamp
- electronic Seals must be admitted as evidence = „Principle of non-discrimination“
- qualified „seal“: „shall enjoy presumption of integrity of the data and of correctness of the origin“
- Not the same legal effects like a qu. electronic signature!
- a qualified electronic seal based on a qualified certificate issued in one Member State shall be recognised as a qualified electronic seal in all other Member States.
- Art. 3 Z 25 and Art. 35 eIDAS-VO

Further Trust Services

- Electronic Preservation Services
- Electronic Validation Services
- Electronic Time Stamping Services
- Electronic registered Delivery Services
- Website Authentication

Legalistic implementation in Austria

BGBI. I Nr. 50/2016

- Federal Law on electronic signature and trust services for electronic transactions (Signatur- und Vertrauensdienstegesetz – SVG)
- Repeal Signature Law (SigG)
- Amend E-Government-Law (E-GovG)
- Logistic adaption of more Federal Laws
- entered into force: **1. July 2016**

Signature and Trust Services Act

Electronic Signature – Specific legal effect for qualified signatures

- A qualified electronic signature meets the legal requirement for the written form in accordance with § 886 of the Austrian Civil Code (ABGB).
- Other statutory or contractual form requirements, particularly those entailing involvement of a notary or lawyer, are not affected (§ 4 Abs. 1 SVG)

Electronic Signature – Exceptions of specific legal effect (§ 4 Abs. 2 SVG)

Qualified signature does not have the legal effects of the written form in the case of:

- Testamentary dispositions
- declarations of intent in family or inheritance law which are bound by the written form or a stricter form requirement *
- a surety bond (Bürgschaft - § 1346 Abs. 2 ABGB) delivered by persons outside their trade, business or professional activity *

* Except the declaration contains a declaration by a notary or lawyer declaring that he or she has explained the legal consequences of the signature to the signatory

Electronic Signature – Consumer Protection

- Explicit Consumer Protection provision in § 4 Abs. 3 SVG
- A business(person) may not exclude the effectiveness of a document signed with a qualified electronic signature by a consumer unless this has been individually negotiated
- Terms of service (Allgemeine Geschäftsbedingungen – AGB) don't fulfill the requirement of individually negotiated

Issuing of qualified certificate

- TSP (or an institution acting on his behalf) has to prove the identity of natural person
- if the person is physically present:
 - by an official photo ID (“Lichtbildausweis”) or
 - verifying by other in its reliability equivalent documented or documented evidence
(Article 24(1)(a) of the eIDAS Regulation)
- if the person is physically not present
 - other methods of identification may be used which offer equivalent assurance with respect to the reliability provided by physical presence (Article 24(1)(d) of the eIDAS Regulation)
 - e.g. “RSa-Brief”

E-Government Act

**citizen
card**

**identity-
link**

mandates

source PIN

**sector
specific
eID**

**source PIN
REGISTER**

**supplement
REGISTER**

**standard-
document
REGISTER**

**official
signature**

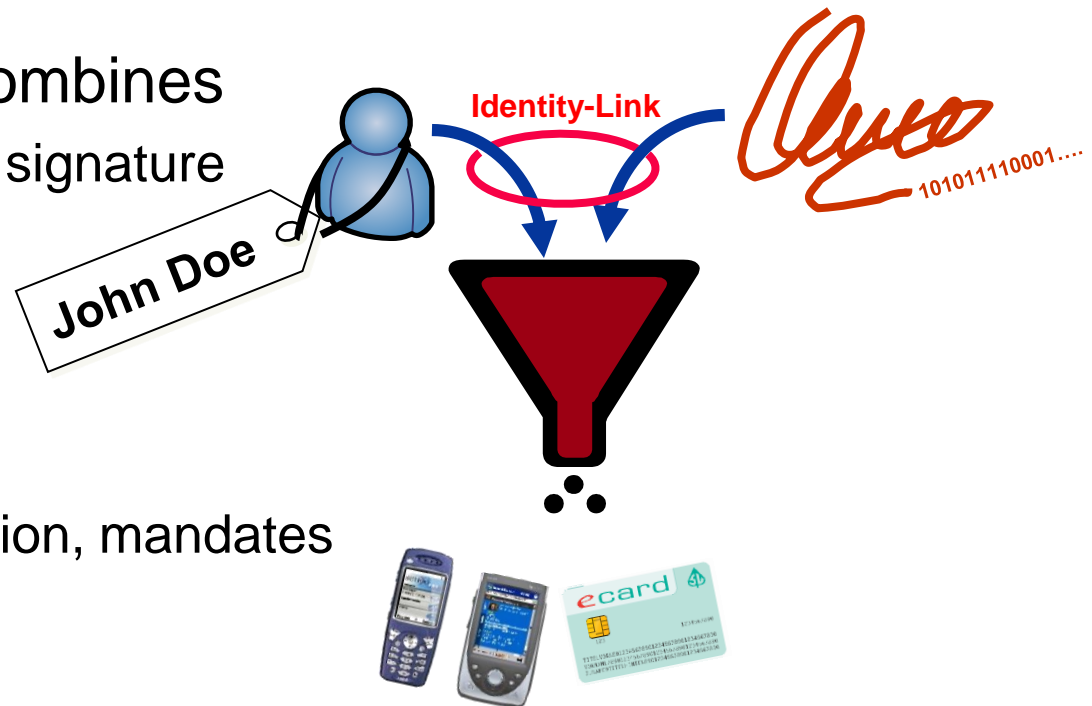
**Register
queries**

E-Government Act

**citizen
card**

eID in AT: the citizen card concept

- The Austrian citizen card is a concept, not a specific technology
- The Citizen Card combines
 - Qualified electronic signature
→ **Authentication**
 - electronic identity
→ **Identification**
 - data on representation, mandates
→ **Representation**



Overview - Austrian Citizen Card

Smartcard



Bank cards
from 2005; ceased



Health insurance card
since 2005



Profession cards, service cards,
...
e.g. notaries, lawyers, ministries,
...



Technology-neutral approach allowed for different implementations

Mobile



A1 signature
service by a MNO
from 2005; ceased in 2008
limited success



Mobile phone signature
Launched end 2009



Defines functions, not the technology

- Identification, sector-specific to enhance privacy
- Qualified signatures, for written form
- Electronic mandates, representation

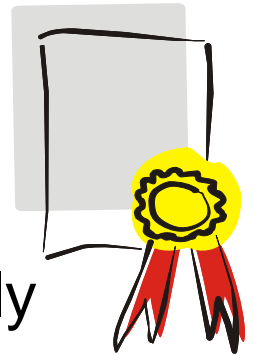
Implementation of this function

§ 4 Abs. 2 E-GovG:

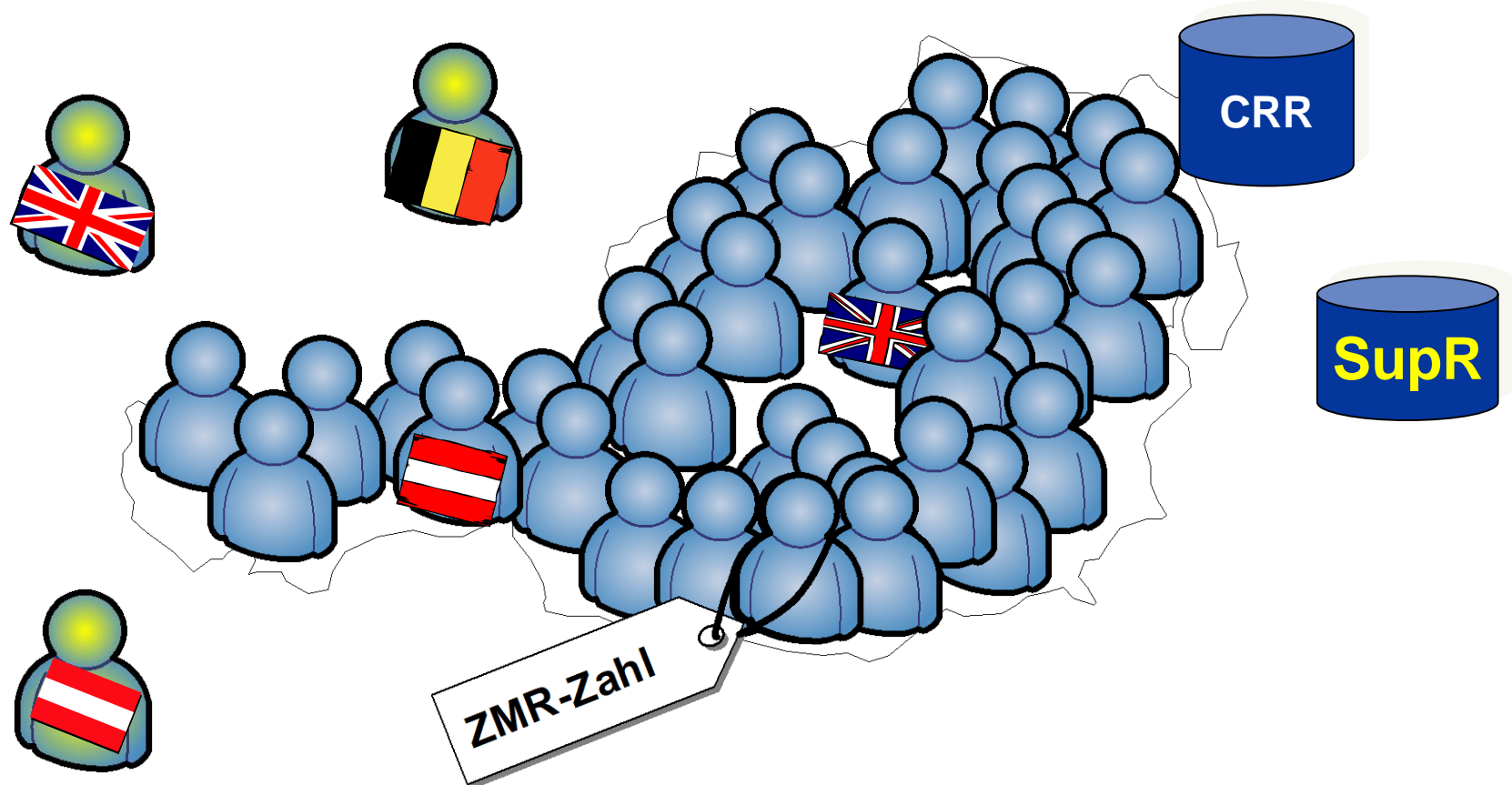
- The unique identification of an natural person results of his/her **Source-PIN**
(= encrypted Number of the Central Resident Register/CRR)

§ 4 Abs. 4 E-GovG:

- The authenticity of the electronically electronically submitted application is provided by means of the **electronic signature**.



Central Register of Residents



Each resident has a unique number (ID) „ZMR-Zahl“ in the Central Register of Residents (CRR)

Sector specific approach in Austria

Austrian eGovernment Act:

Base register(s)



SourcePIN



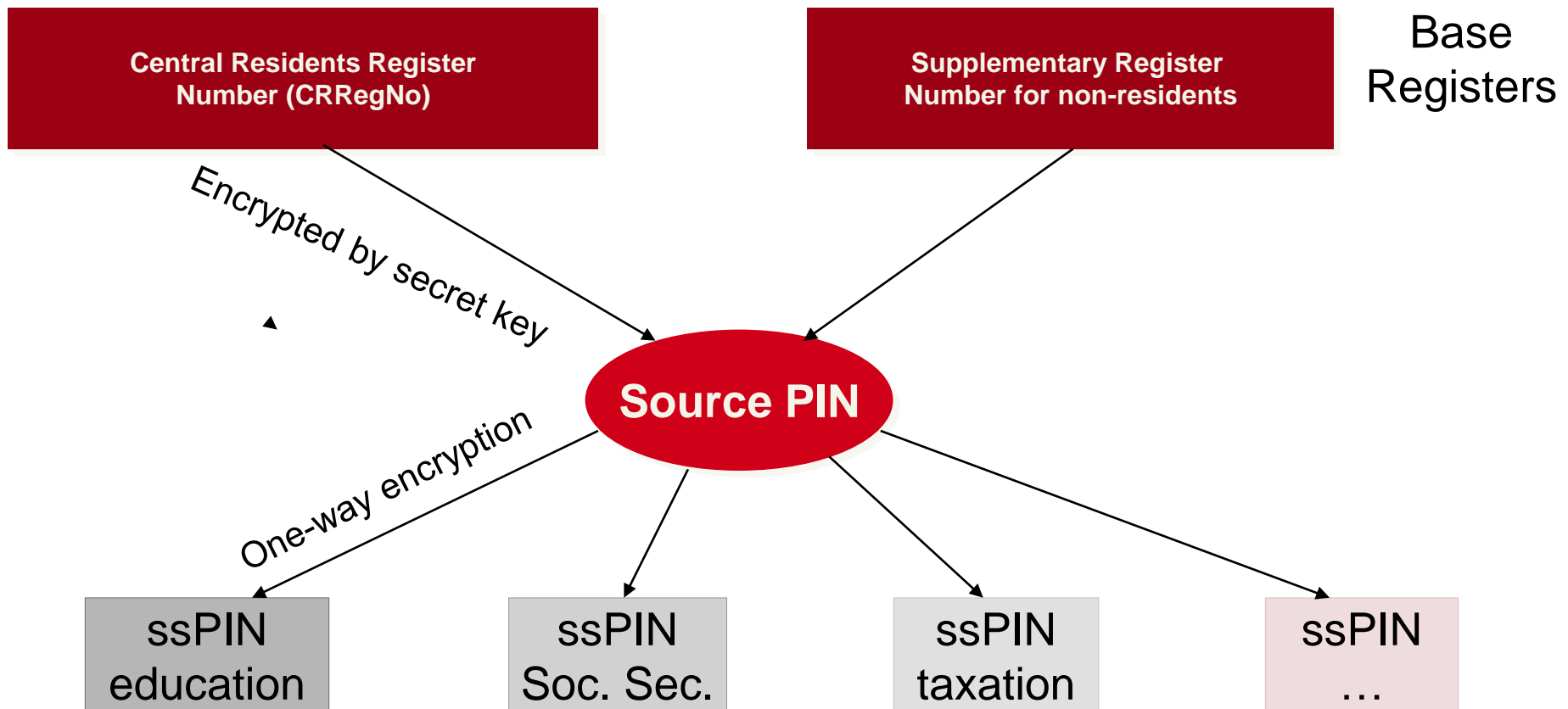
Sect.spec.PIN

The base registers provide for unique identification

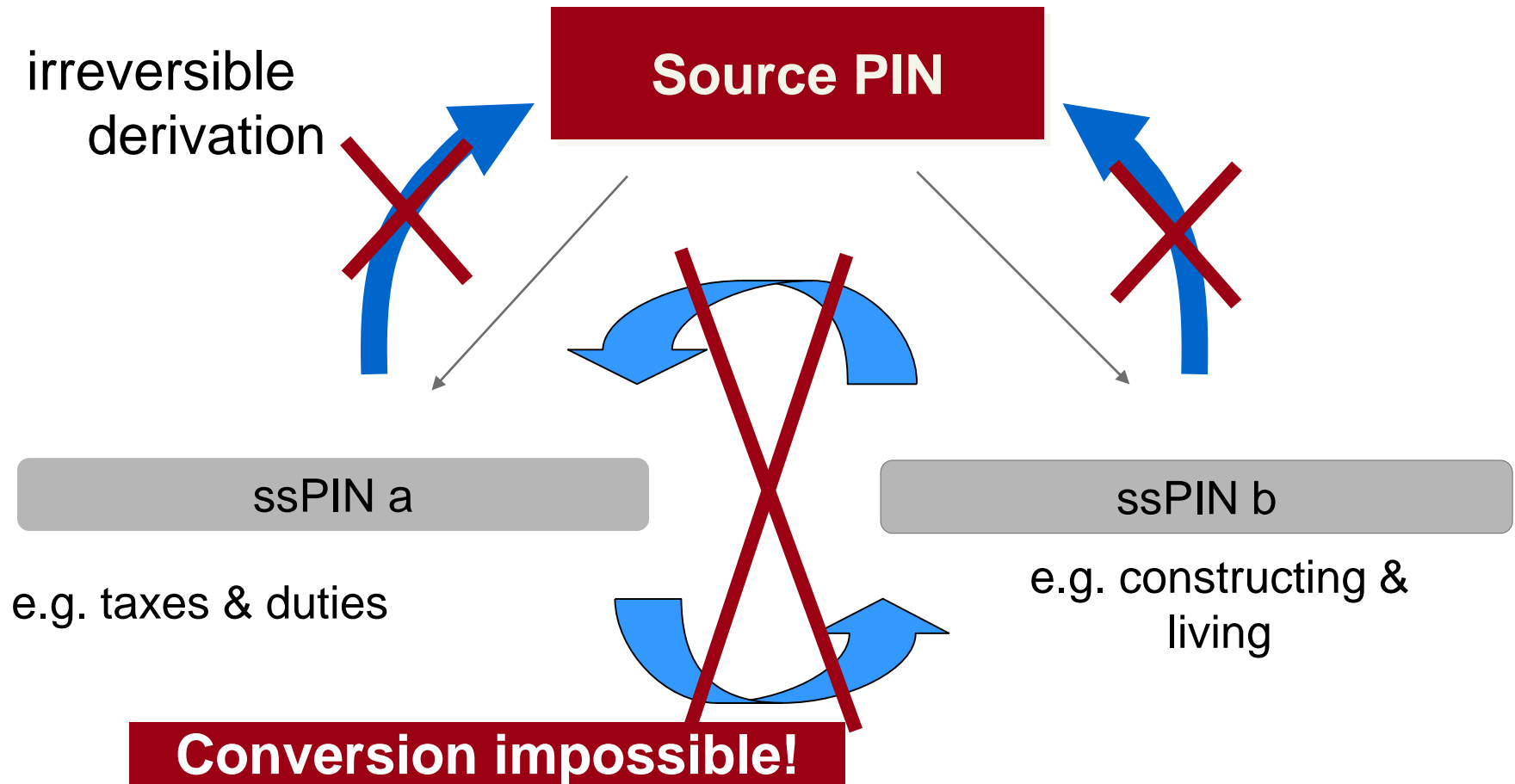
The SourcePIN represents the uniquely identified person; it is a hidden number, stored only in the Citizen Card, which is in the possession of the data subject

In government data bases only the appropriate sector specific PIN appears for identifying data subjects

Electronic identity of natural persons

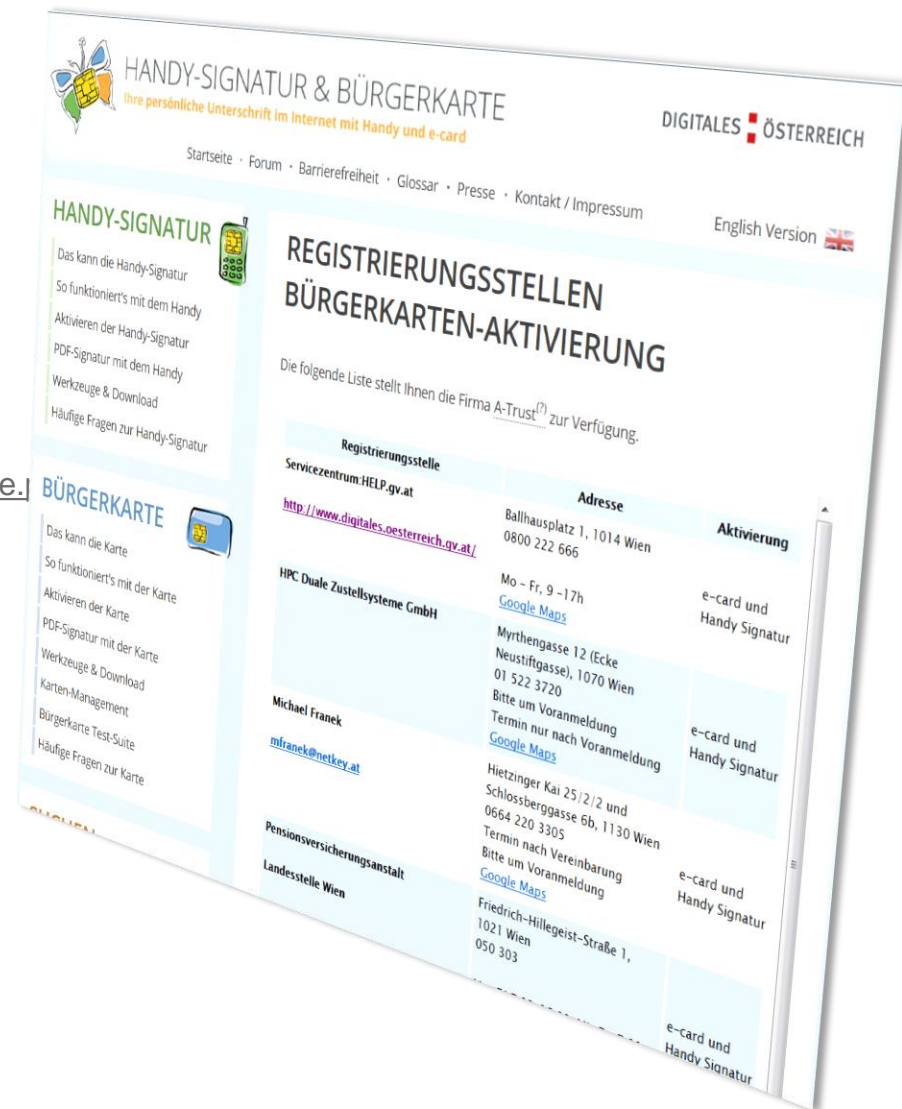


ssPIN: Generation



Registration

- Registration offices
 - All tax offices
 - Many municipalities
 - Many regional entities
 - Social security offices
 - Schools
 - <http://www.buergerkarte.at/registrierungsstellen.de>
- Online Registration (+ postal delivery of activation code)
 - via FinanceOnline
 - via Post.at
 - via online banking
 - www.youtube.com/watch?v=qBBafPdi-hY
- „Self Registration“ using a qualified signature (existing citizen card):
 - <https://www.handy-signatur.at/>



Outlook: E-GovG amendment 2017

E-Government Act

„new citizen
Card“ = eID

Citizen Card „new“ by E-GovG-amendment

- Change of terms
 - „**Elektronischer Identitätsnachweis (E-ID)**“
instead of „Citizen Card“
- Official process for the **registration** of an E-ID:
 - Registration of an E-ID (Identification) in the context of the application for a passport at the passport authority
- Extension of the functional scope of the E-ID, in particular by the inclusion of **further attributes**:
 - Proof of data from registers of public sector (such as civil status register, resident register, driving license register)
 - Access to such features only with the consent and knowledge of the person concerned

Transitional provision

- Start of application of the law not until there are technical/organizational requirements for real operation E-ID-system established
- Until the start of the application of the law ("real operation E-ID"), existing citizen card system remains applicable

E-Government Act

official
signature

„Official signature“ of documents

Bundespolizeidirektion Wien
Strafregisteramt

Wasagasse 22
1090 Wien

Gebühr entrichtet

BEZUG: SB INTERNET SRB2008072509213901
(REFERENCE NUMBER)

STRAFREGISTERBESCHEINIGUNG
(CRIMINAL RECORD CERTIFICATE)

Familienname(n): Kustor
(Family Name)

Geschlecht: männlich
(Gender: MALE)

Vorname(n): Peter Michael
(First Name)

Akad. Grad: Mag.
(Academic Degree)

Geboren am: 24.06.1970
(Date of Birth: DD.MM.YYYY)

Geburtsort: Wien
(Place of Birth)

Im Strafregister der Republik Österreich - geführt von der
Bundespolizeidirektion Wien - scheint keine Verurteilung auf.
(No convictions are listed in the criminal records database of the
Republic of Austria, kept by the Federal Police Directorate of Vienna.)

DVR: 0003506

Tagesdatum: 25.07.2008
(Date)

Uhrzeit: 14.48.37
(Time)

Verfahren	urn:publicid:gov.at:form-srb-1.1
Datum	2008-07-25T12:48:52
Aussteller	CN=s-sign-corporate-light-02,OU=s-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
Seriennummer	82210
Signaturwert	R6Dulb0uXklJdu/NT936Y41quG4DLsTazoCvo5ovcCdrhRX/0amVnAGQAYjiTFWm9Tc0NihpK06SQ/ERisxfczSo7HM6zdu2Py8.84j1fBcvRzKVM/YbB2kK6YUjxxdG3MDikOi2nUS6ZTqklUEWEKkPqKmhCLv4kGBgfB8levo-

Prüfinformation: Informationen zur Prüfung der elektronischen Signatur finden Sie unter:
<https://apps.gsis.gv.at/srb-vnr2>

Hinweis: Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß §20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.

- It facilitates recognition of the fact that a document originates from an authority
- It has to be visualized with certain elements

Official Signatur (Amtssignatur)



- only for signing by of the public sector
- at least “advanced” electronic signature or seal, depend on natural or legal person is certificate holder
- The signature / seal certificate includes a specific attribute, which only the public sector is allowed to use
- authority may act as creator of a seal
- Official signature can be based on software-based server certificate, because of “advanced” or seal

Different implementations rgd visualization

Minimum content:

- logo of the authority
- Explicit information that it was “officially signed”
- Information needed for the verification of the electronic signature and the printout

Signaturwert	LF0bBxaQvybBYuzAFMr0C3LuSBBDnz2knSA22A+6K6M8Ur37KCoG8OWSR0cQ2hU4uPw97qpUs1nmmWJC8TpMqb9sX8BVSvS9m9T1bjQ0jfnPFkhl1We9gBzjU5C1WjpP//Bq4ZgcaFfdj1ZgskWuSQ1V56G+mZz1PyKai7iFfZjx0GeX49V8hVklZk+QJaks0oIJMqEypKjZyAHQ4FuLMch3+YIfytE/u5bfbjYbXrPo6iZaTMVXOHjYPCu9qD6IfglS6/fZpaDdTZLQaniiYqa6LXX827WzLQ9Q27Z0aTgld5jbVKt6D1UmpPpOH/LU5QAiC5jiHW72f60GIwRH1w==	
	Unterzeichner	BMI SU-ZMR
	Datum/Zeit-UTC	2010-09-07T14:08:30+02:00
	Aussteller-Zertifikat	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serien-Nr.	450207
	Methode	urn:pdfsigfilter:bka.gv.at:text:v1.2.0
	Parameter	etsi-bka-moa-1.0
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: http://www.signaturpruefung.gv.at . Zur Prüfung des Ausdrucks senden Sie bitte einen Scan an zmr-clearingstelle@bmi.gv.at	
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß § 20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

Dieses Dokument wurde amtssigniert.

Informationen zur Prüfung der elektronischen Signatur und des Ausdrucks finden Sie unter: <https://www.wien.gv.at/amtssignatur/>

Dieses Dokument wurde amtssigniert.

Informationen zur Prüfung der elektronischen Signatur finden Sie unter <http://www.signaturpruefung.gv.at>

Die Echtheit eines Ausdrucks kann durch Vorlage beim Absender verifiziert werden. Details siehe: <http://e-government.bgld.gv.at/amtssignatur>

	Datum/Zeit-UTC	2012-05-21T15:19:03+02:00
	Hinweis	Dieses Dokument wurde elektronisch signiert. Auch ein Ausdruck dieses Dokuments hat die Beweiskraft einer öffentlichen Urkunde.
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur und des Ausdrucks finden Sie unter: http://kundmachungen.justiz.gv.at/justizsignatur .

Signature (seal) validation

Follow the **link** in the individual document for information or go directly to the **signature verification service** of the AT Supervisory Authority for electronic signatures (seals)



www.signature-verification.gv.at

The verification procedure and result

Verification report

Document	
File name	2016 Strafreisterbescheinigung.pdf
Hash value	rQW11pE5SmhWMW9APiv87nmfOc= (SHA-1, Base64-encoded)
Size	128.83 kB
Type	PDF signature (PADES)

Signature	
Checks	
Time of signature and verification resp. (UTC)	2016-08-04T06:19:30Z
Signature Certificate	The verification of the signature value was successful. There is a certificate chain up to a trusted root certificate. Each certificate of this chain was valid at the given time.

Further information	
Type of signature	PADES
Annotation	The certificate fulfills the technical requirements for official signatures.

Signer	
Name	BMI-TRUSTCENTER
Organizational unit	BMI
Organization	GV
Country	AT
Serial number	dec.: 145680069260, hex.: 21:eb:35:72:8c

Issuer	
Name	a-sign-corporate-light-02
Organizational unit	a-sign-corporate-light-02
Organization	A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH
Country	AT

Certificate	
Serial number	dec.: 1624172, hex.: 18:c8:6c
Quality	official signature certificate
Validity period	valid from 2015-06-24T08:50:17Z to 2020-06-24T06:50:17Z The given time of verification is within the validity period.
Attributes	administrative capacity
Key usage	digitalSignature, keyEncipherment, dataEncipherment
Certification policy statement	http://www.a-trust.at/docs/cpi/a-sign-AmtsSignatur

Note: Under the Austrian Signature Law, Austrian certification service providers that issue qualified certificates are under supervision of Telekom-Control Commission. Its branch Austrian Regulatory Authority for Broadcasting and Telecommunications (RTR) offers this signature verification service. Electronic signatures based on certificates issued by foreign certification service providers offer an automated verification; in that case no guarantee whatsoever for a correct technical interpretation of such foreign certificates can be given.

Signature Value	
Signature	Signature Verification v1.0.1
Issuer-Certificate	CN=RTR Services 3, O=Bundfunk und Telekom Regulierungs-GmbH, C=AT
Serial-No.	2
Method	urn:pdfsigfilter:bka.gv.at:bsigner-v1.1.0
Parameter	etcl-bka-mob-1.0
Verification	Information about the verification of the electronic signature and of the printout can be found at: https://www.signature-verification.gv.at/
Date/Time-UTC	2016-08-04T11:32:09+02:00

- Upload doc.
- See:
 - Signatory
 - Verification successful
 - Valid certificate chain
- Link to detailed and signed report (see picture left)
- Service uses the EU Trust List (eIDAS)

Probative Value of Printouts (§ 20 E-GovG)

- electronic official signed document is always considered as original = authentic public document (öffentliche Urkunde)
- also an electronic document of an authority (e.g. “Bescheid”) printed out on to paper is assumed to be authentic (§ 292 ZPO)
- regardless of whether authority or recipient prints the official signed document

Documents issued by Public Authorities

- § 18 of the General Administrative Procedure Act 1991 (AVG) foresees that (since 1.1.2011)
 - Official documents issued **electronically** have to bear an **official signature** (§ 19 E-GovG)
 - Official documents issued on **paper** have to be
 - **manually signed** by the official approving the document or
 - manually **certified** by the office, indicating that the document corresponds with the document approved by the responsible official or
 - the paper document is the printout of an electronic document which bears an **official signature**. In this case, no further requirements need to be met.

General Administration Procedure Act (AVG)

Submissions/Applications (Anträge)

- Submissions may be filed in *writing*, *orally* or by *telephone* (§ 13 Abs. 1 AVG)
- *Written* submissions may be communicated to the authority in any technically feasible form
- by *e-mail* however to the extent that no specific means of communication are provided for the electronic communication between the authority and the persons involved. (§ 13 Abs. 2 AVG)
 - e.g. e-form
- From 2020: Everyone has the **right to electronic communication** with the courts and administrative authorities (in matters which are federal law in legislation) (§ 1a E-GovG)

Submissions/Applications (Anträge)

- Eventual *technical* requirements (file format, interfaces) or
- *organisational* restrictions of the electronic communication between the authority and the persons involved (time limitation, certain e-mail-address)
- are to be published in the internet
 - is no enabling provision, but merely a publicity requirement for any organizational restriction (VfGH-Erkenntnis 106/2013-10 vom 3.3.2014)
 - Sending an application to an other e-mail-address than the published, bears the risk of loss or of delay of the application

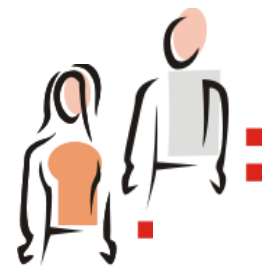
Submissions/Applications (Anträge)

- the authority is obligated only during office hours to accept submissions in writing or
- operate receiving appliances (Fax!)
- the office hours and the hours for the public are to be published in the internet (§ 13 Abs. 5 AVG)
 - AVG links only to the organizational set office hours and their publication in the internet
(VfGH-Erkenntnis 106/2013-10 vom 3.3.2014)

Service of documents (delivery act)

Electronic Delivery (Zustellgesetz)

- transmission of documents in execution of the laws (§ 1 ZustG)
- not applicable for private sector
- different regulations for finance authorities (Finanz Online!) and
- courts of law (ERV – Elektronischer Rechtsverkehr für Gerichte)



4 Types of electronic delivery (ZustG)

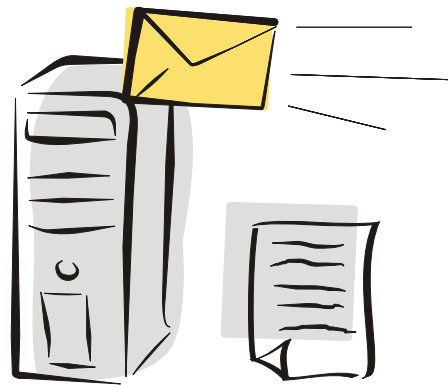
1. delivery to an electronic delivery address (e-mail)
 - without proof of service
2. via the electronic communication system of the authority (§ 37 ZustG)
 - without proof of service
3. immediate electronic release (§ 37a ZustG)
 - without proof of service except citizen card was used for logon

4 Types of electronic delivery (ZustG)

4. e-Delivery via electronic delivery service providers (§ 35 ZustG)

- delivery **with** proof of service (like Rsa/RSb in paper)
- delivery confirmation through using the qualified electronic signature of the citizen card
- citizen card is mandatory
- service provider are authorized (§ 30 ZustG) and
- supervised (§ 31 ZustG) by the Minister for Digital and Economic Affairs

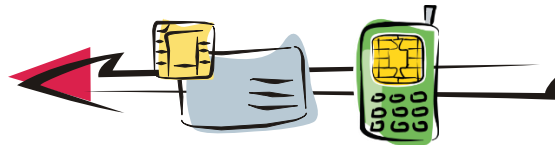
e-Delivery via electronic delivery service providers



1) document transmitted by administration



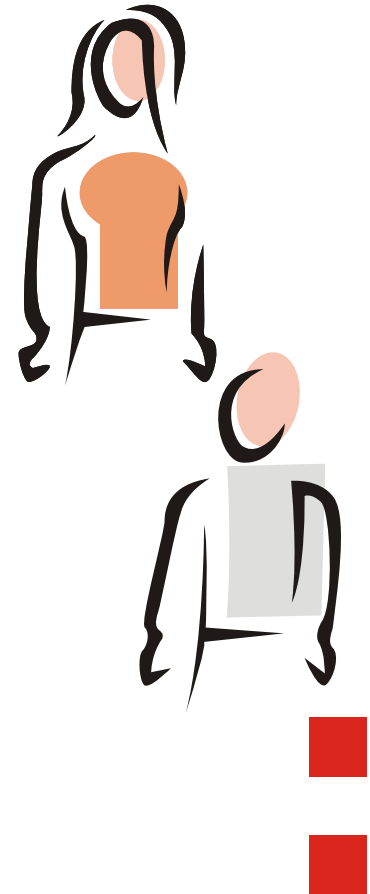
2) eMail notification



**3) eID and signature based login
(to confirm receipt)**

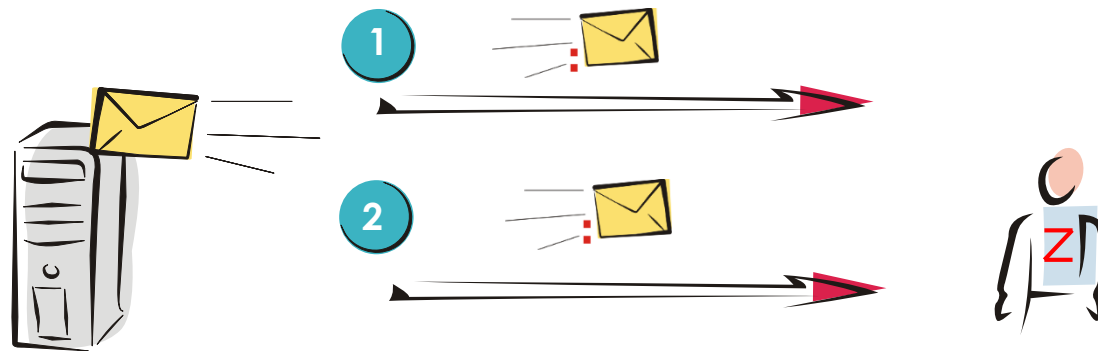


4) deliver document content



e-Delivery via electronic delivery service providers:

Notification through delivery service provider



1. Electronic notification (immediately to all electronic addresses)
2. Electronic notification (if the document is not picked up within 48 hours)

e-Delivery via electronic delivery service providers: delivery effect (Zustellwirkung)

- Document is at the latest considered as delivered when picked up (§ 35 Abs. 5 ZustG)
- else on the first workday after the electronic notification has been sent (§ 35 Abs. 6 ZustG)
 - Saturday is no workday
- Document is considered to be delivered without being picked-up by the recipient

e-Delivery via electronic delivery service providers: Exeptions of delivery effect

- No delivery effect, if
 - the electronic notification was not received by the recipient, but delivery will take effect on the day following the electronic notification is received within pick-up period (14 days). (§ 35 Abs. 6 2. sentence ZustG),
 - the recipient of the electronic notification had no knowledge of the notification or
 - the recipient was aware of the notification, but was not merely temporarily absent from all delivery points during the pick-up period, delivery will take effect on the day following the return to one of the delivery points within the pick-up period at which the document could be collected. (§ 35 Abs. 7 ZustG)

Display module / Anzeigemodul § 37b ZustG

- Bundles documents from different delivery systems
 - Electronic Delivery Services
 - electronic communication system of the authority (§ 37 ZustG),
 - ERV,
 - FinanzOnlinein common view.
- Delivery systems introduce meta-information into the display module, which is then displayed
- Documents themselves remain with the respective delivery system
- it is only accessed via the display module



mandatory participation in electronic delivery for companies

- § 1b E-GovG idF BGBl. I Nr. 40/2017 (DRG 2017)
- **Companies** have to participate in an electronic delivery system
- At the latest **1.1.2020**
- Display modul (§ 37b ZustG) for bundled view of all documents.

Thank you

for your attention!

Mag. Gregor Schmied
Bundesministerium für Digitalisierung und
Wirtschaftsstandort

