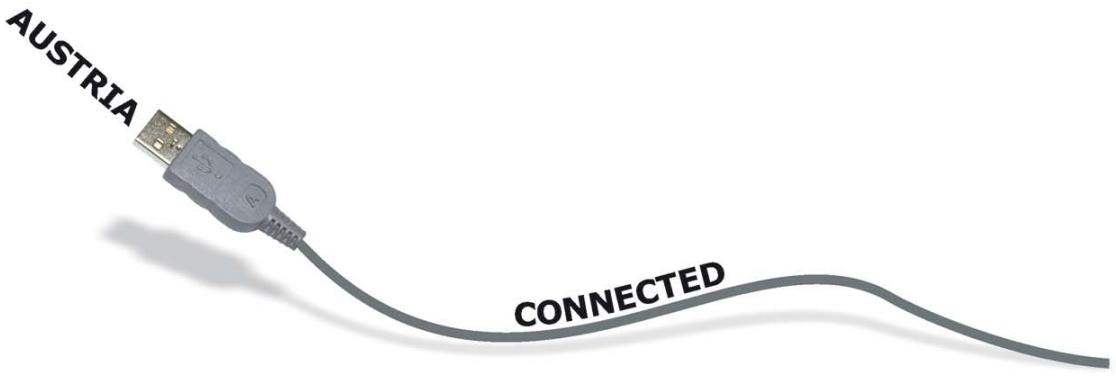
DIGITAL AUSTRIA

Administration on the Net

The ABC guide of eGovernment in Austria

New Edition 7/ 2008



FEDERAL CHANCELLERY AUSTRIA

July 2008

Imprint:
Austrian Federal Chancellery,
ICT Strategy Unit
A-1014 Vienna, Ballhausplatz 2
E-mail: ikt@bka.gv.at
Agency responsible for content: Austrian Federal Chancellery
Editors: Gregor Eibl, Christian Herwig, Bernhard Karning, Peter Kustor, Peter Reichstädter, Christian Rupp, Martin Spitzenberger

Administration on the Net
The ABC guide of eGovernment in Austria

Preface

eGovernment leverages information and communication technology to strengthen and improve the quality and efficiency of public administration. Communication is made easier for citizens and businesses, costs are lowered and at the same time internal processes are sped up substantially. The quality and transparency of public services is raised considerably to everyone's benefit. Simply put, eGovernment has become a synonym for a modern state.

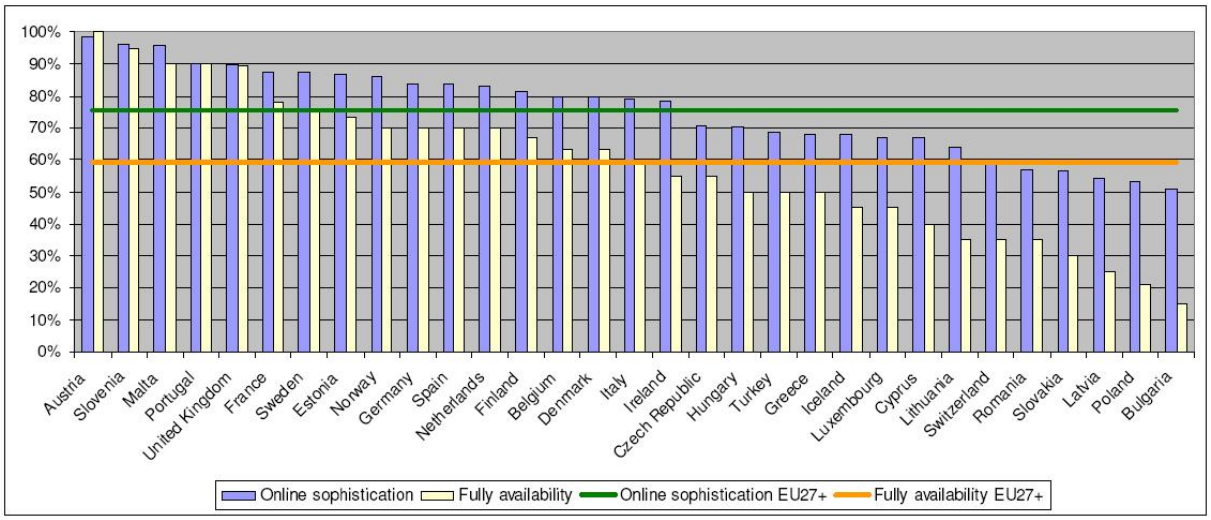
The development and implementation of electronic public services is one of the priorities of the Austrian Federal Government. The government plan principally states that every citizen in every community should have access to all forms of eGovernment at the federal, provincial and local levels. Secure communication and transactions and confidential handling of personal data have top priority.

International services are an important instrument for supporting mobility in the home market and European communities. The EU Commission has also recognized this and has therefore given eGovernment high priority in the i2010 program. Therefore, special care must be given to make sure that electronic services are able to meet the needs of all citizens in different countries.

In the last few years, Austria has become the showcase for electronic offerings for many other countries. The management and information technology consulting company, Capgemini, was commissioned for the seventh time by the European Commission to investigate eGovernment offerings in 25 EU Member States as well as Iceland, Norway and Switzerland. During the eGovernment Conference of Ministers in Lisbon on 20 September 2007, Austria

was declared the European champion in eGovernment for the second time in a row.

Starting at 13th place in 2002, Austria has been able to continually work its way upwards since then. These achievements are even more noteworthy considering that Austria was able to raise the bar and make additional improvements in both study categories in 2007 despite the high standards it had already reached. The online sophistication[1] of base services in Austria is measured at 99% and all services were graded level 4 or 5. This means that, according to the indicator, 100% of online capability has been achieved.



The 2007 study was distinguished by a series of innovations. This made it necessary to introduce a fifth level to the assessment criteria in order to take user orientation into account - a criterion which the Austrian eGovernment services fulfilled excellently. Amongst other new changes this year were the separate analyses of a national portal and the application of electronic identification mechanisms.

---

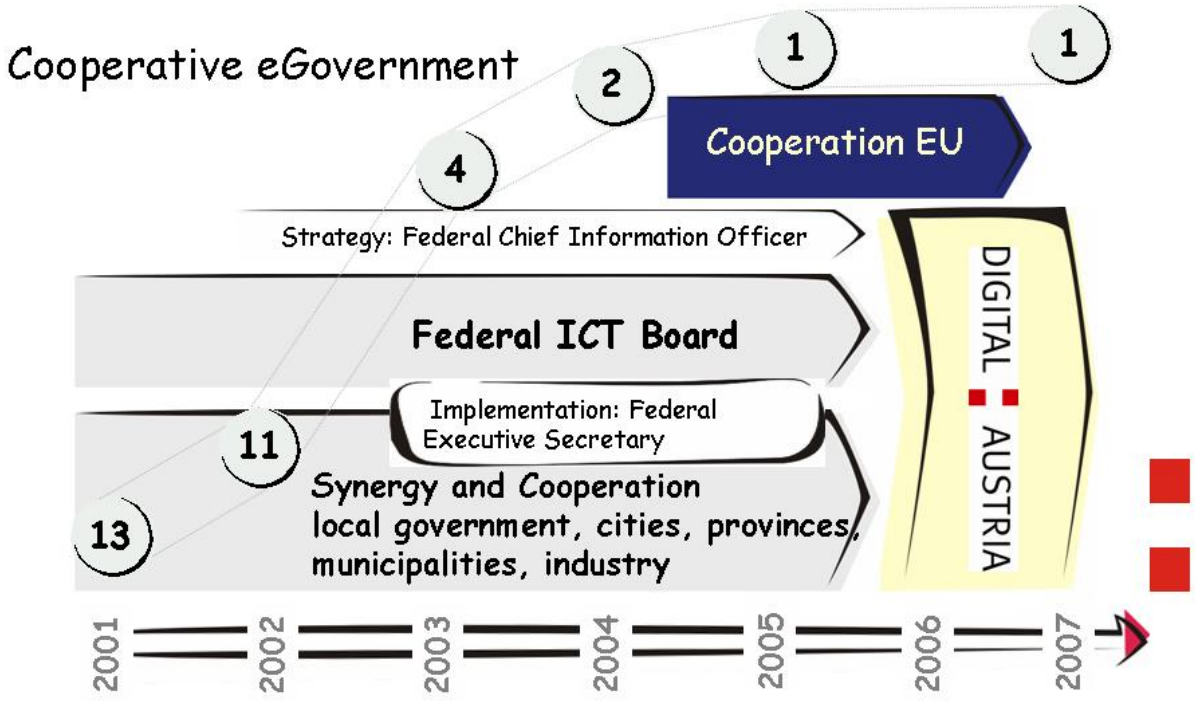
[1]In Benchmarking tests, 20 base services were defined, 12 for citizens and 8 for businesses. These were used to measure progress in the implementation of e-government in the more than 14,000 public administration Web sites that were analysed. The sophistication of each service is judged on a 4 or 5 level scale, starting from the net amount of information, to procedures that can be conducted completely online. In addition, they are also judged on the percentage of services that can be carried out competely online. Those services that achieved this are awarded the highest level.

The HELP.gv.at site as a "one-stop shopping" portal and the application of the citizen card as a uniform system of electronic identification in Austria contributed significantly to its success. Entire procedures are able to be carried out electronically without changes in the type of media (e.g., switching between electronic and paper format), starting from filling out an application form and paying fees, to internal processing (ELAK) and delivering official documents and notifications.

The eGovernment Act, which came into effect on 1 March 2004, forms the legal foundation for electronic communication with public bodies. Through cooperation with Industry, all bank debit cards (Maestro with a-sign premium and Mastercard) and all health insurance cards (e-card) have been equipped with citizen card functionality since end of 2006. The high level of security and data protection has been affirmed many times through numerous international awards.

The use of electronic services from public authorities is also rising steadily. According to Fessel-GfK, 80% of the people gave eGovernment a positive rating, and more than 45% have already completed application forms electronically - an increase of more than 137 percent points within three years. Nowadays, 80% of Austrian Internet users prefer to use the Web for conducting business with public authorities rather than going in person to a public administration office. More than 60% would prefer to receive official notifications in electronic form rather than receiving them by post.

The Federal Platform Digital Austria was founded in 2005 by the Austrian Federal Chancellery as country-wide platform to help coordinate on a uniform eGovernment strategy for the Federal Government, the provinces, municipalities and local authorities and businesses. Through the integration of public administration bodies at all levels, i.e. federal, provincial, municipal and local levels and in cooperation with businesses, all projects, strategies and guidelines are collectively planned, coordinated on and implemented. This was and is one of the most important factors behind Austria's success in eGovernment internationally.



This document introduces eGovernment and its advantages to citizens, business people, and public administration according to target groups. Lawyers and technical engineers alike will find information of interest in the new edition of the ABC guide of eGovernment document in the newly added chapters.

The book "**Administration on the Net – the ABC guide of eGovernment in Austria**" serves as an accompaniment to users for eGovernment applications and equips them with digital know-how.

The Austrian eGovernment strategy is based on basic concepts, base components and (open) standards, which serve as guidelines for the implementation of electronic services and the creation of the underlying infrastructure. Austria is among the pioneers in this area and many of our solutions serve as a model for public authorities in other nations. The "**Best Practice Catalogue – eGovernment in Austria**" presents tools and applications that could be made available immediately to other nations to aide them in their eGovernment endeavours.

Your,
Federal Platform Digital Austria, Austrian Federal Chancellery

Introduction

eGovernment Basics

Computers, mobile phones, Internet: we live in a thoroughly technical and technological society and are, without our noticing it, completely surrounded by technology. Mobile networks and the Web are our “new” communication systems, without which our society would not be able to function. It would be impossible to imagine not being able to make mobile phone calls, or send messages worldwide in a matter of seconds by e-mail or to retrieve information from the Web with only a few clicks.

But it’s not just citizens who are living a digital lifestyle. Public administrations and authorities are also fully embracing information technologies in order to communicate in modern ways. The term eGovernment was already coined years ago to describe this concept.

The Definition of eGovernment

The word eGovernment translates literally as "electronic government". However, the term eGovernment has established itself worldwide as meaning "the administration of government by means of electronic technology”. In general, it means the simplification of work routines and processes through the application of information and communication technologies in the areas of information administration, communication and transactions within and between state institutions as well as between the government and citizens or businesses.

eGovernment is classified into the following areas:

- Information: Making information available online, for example, on the Web site of a public authority.
- Communication: The ability to interactively access and exchange information.
- Transaction: The actual carrying out of services, including the signing of application forms and electronic delivery of official documents and notifications.

eGovernment is the set of all electronic public administration services available to everyone in the country. It is also a synonym for a modern and innovative land, in which quality, trust and quickness plays a central role.

Public administration and authorities use technologies such as the Internet or mobile services to get into contact with citizens and businesses. They also use these technologies to carry out internal work processes. eGovernment has an impact on every citizen, business and public authority.

Modern information and communication technologies (ICT) make it possible for public authorities to offer "old" services as well as introduce new electronic ones over the Internet. Not only can these services be customised to meet the needs of citizens and businesses, they also make life simpler. Many of these services save people from having to go to the public office in person because application forms can be sent over the Internet. The use of communication technology allows citizens and businesses to communicate interactively with public authorities. The World Wide Web is practically open around the clock, which means that applications and forms can be sent to the electronic public authority any time of day or night. eGovernment also helps the government to reach new levels: historical processes and forms are reassessed, brought up-to-date where necessary, or even disposed of entirely.

However, eGovernment does not mean that traditional offices are done away with entirely. Although transactions with public authorities can be conducted over the Internet, it doesn't necessarily have to be done that way. For all those who prefer personal contact or those who are uncomfortable using the Internet will still be able to go to the public office in person.

eGovernment Principles

The Austrian eGovernment strategy is based on the following important principles:

Proximity to citizens

Government should be at the disposal of the people and not the other way around. Online services need to be easy to find and available at all times.

Convenience through efficiency

Online processes should make life simpler and more convenient: not having to show up in person, no closing times, no waiting in line, or being sent back and forth between offices, just uncomplicated processes and "intelligent forms" that are logically designed and can be filled out intuitively, or even pre-filled with the necessary information. Processing forms using an automated system also optimizes work processes in public authorities.

Trust and security

Citizens have to be able to trust the electronic public authority as much as they do the traditional one. A citizen must be able to verify that electronic versions of official documents they receive have not been altered and that they really were sent by the proper authority. Conversely, public authorities are able to check if the documents received from citizens arrive in their original state and that they are really sent from the given person.

Transparency

New technical developments will only be accepted if all those affected by it, from employees in public authorities to those in business, are involved in the process and developments are carried out in a transparent fashion.

Accessibility

Public authority services must be accessible to everyone without discrimination. eGovernment must be available to all classes and sections of the population. A "digital divide", meaning a separation between those who are comfortable using new technologies and those who find it difficult, must not be allowed to exist. The solutions offered as well as the Web sites themselves must be barrier-free and accessible to all. Additional solutions, such as public Web terminals, should make it possible for everyone to be able to use eGovernment.

Usability

The range of electronic services offered must be structured in an easily comprehensible, clear and straightforward manner. In order to gain acceptance and approval from users, forms and portals will have to have a consistent design. Navigation and menus will need to be intuitive and logical, with a familiar structure so that users are able to quickly find what they are looking for.

Data security

Citizens place a high degree of confidence in the Austrian administration with regard to data protection. Citizens put a high value on the protection of their privacy. Sector-specific personal identifiers, or ssPINs, were developed specially for the purpose of identification to conform to data protection standards. They ensure that only authorised persons within the administration have access to personal data.

Cooperation

eGovernment functions best when all levels of government work seamlessly together, from the smallest local authority up to federal ministries. Existing applications and infrastructures will have to work together in order to reach the desired level of efficiency. Only through cooperation will it be possible for eGovernment to run in an efficient manner; organisationally, financially and administratively. The basis of this cooperation are interfaces that government agencies jointly develop and present to the public.

Sustainability

eGovernment has a modular structure which allows new components to be integrated immediately into the system to keep up with the latest technology. A modular structure offers more than just sustainability – it also increases Austria's ability to compete in the market and strengthens its position as a location for business.

Interoperability

Diverse types of systems will need to be able to communicate with each another. Therefore, eGovernment solutions will only be

designed according to internationally recognized standards and open interfaces.

Technological neutrality

The speed with which systems, solutions and devices are developed in the information and communication branch is faster than any other area. Products that are new today are already outdated tomorrow. eGovernment must therefore be open to new developments and not insist on only using one particular technology. It must not allow itself to become dependent upon a specific software or hardware monopoly.

Which Needs Should eGovernment Fulfill

eGovernment works best when all citizens and as many areas as possible are involved in the process. It should enable businesses and citizens to make enquiries and file applications electronically, receive comprehensive information online, and make it easier to conduct transactions with public authorities. Special emphasis must be placed on customer orientation.

For citizens, eGovernment means being able to apply online for various services and documents such as grants, income tax forms or criminal record certificates. Some documents, like the residential registration form, will become obsolete because authorities will be able to exchange information electronically with each other directly.

For businesses, eGovernment means being able to fill out applications online for the Business Registry and pick up their registration certification when it is completed. It means being able to get their questions on local taxes or foreign trade answered over the Internet. Information on company insurance or new amendments to the city, country or EU laws should also be able to be researched.

For public authorities and government, it means optimizing work processes in areas such as construction management, electronic customs clearance, and materials and electronic file management through the application of new technology and

communication systems. eGovernment is both the present and the future.

eGovernment will do more than just improve services, save costs, make work processes more efficient, and enable independent work. It will also make communication between citizens and businesses and the government more transparent, and open up new possibilities for the way information is presented and accessed. One of the most important promises is that it offers more opportunities for participating and having a voice in community matters. eGovernment makes this possible because it is the basis for e-democracy: a living electronic democracy. If desired by the majority of the population, in the future we will be able to use modern communication devices such as mobile phones and the Internet to share our opinions and cast our vote in electronic referendums and elections. E-democracy results when communication between citizens and legislative and state institutions is simplified. But above all, eGovernment means being closer to the common people.

Many new opportunities

eGovernment got an early start in Austria. Since its begin in 1998, public authorities and eGovernment project teams have continually been working to expand and improve on public services. eGovernment solutions have improved communication between public authorities. New services are constantly being developed and existing procedures are being improved and modernised. There are already several procedures that can be carried out completely over the Internet, such as filing for a tax return. Austria is not only a forerunner in the EU; it also serves as a global example for the way eGovernment could and should function.

The right strategy

A successful eGovernment needs well-informed citizens, businesses and public authorities who work with eGovernment and realise new electronic developments. This is only possible with the right strategy. The Austrian eGovernment strategy outlines basic concepts, base components and new standards which serve as guidelines for the implementation of electronic services and its infrastructure. Only with the right plan can a state convert its

government into a citizen and business-oriented eGovernment. As seen in the Figure below, this plan is comprised of various components. Each individual area represents an important building block in a virtual eGovernment structure.

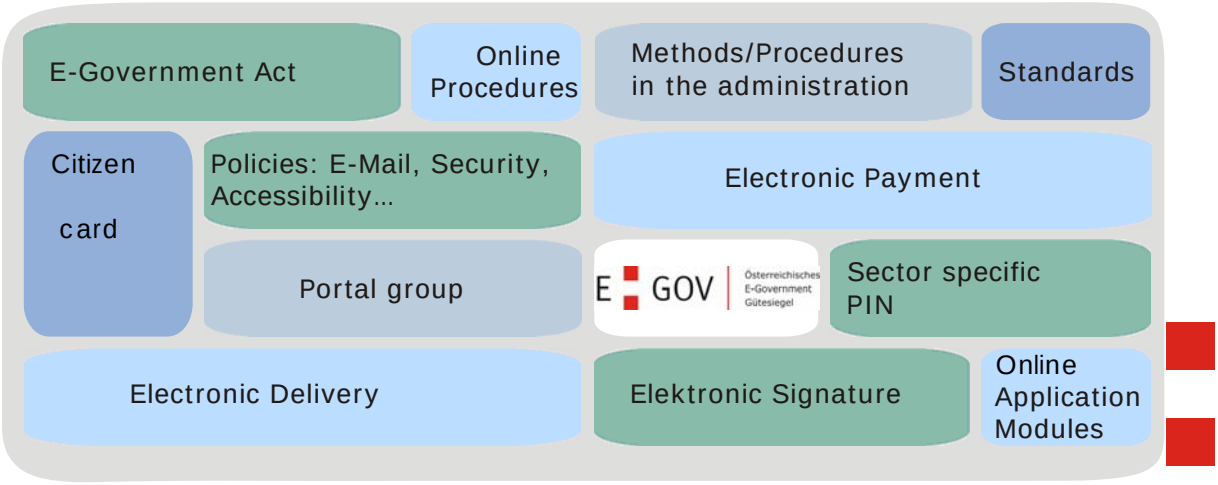


Figure 1: Areas in the eGovernment strategy

Even though eGovernment has been a topic since 2001, there is still much left to be done. In fact, eGovernment is a living system that constantly grows, learns and improves itself. Citizens and businesses continually breathe new life into it by using it and growing with the system.

eGovernment should also be viewed on a European-wide scale. In an increasingly global world, the EU and its institutions must put eGovernment and its advantages to use for its approximately 500 million citizens and businesses, so that they can communicate and interact electronically with governments across all borders.

History and Organisation

How Is eGovernment Organised in Austria – Who Is making Austria Digital

The decision to go ahead with a cooperative eGovernment endeavour came in Austria in 1998. The task force "E-Austria", made up of leading experts in Austria, recommended instituting an "ICT Board", which would be responsible for coordinating planning and implementation of eGovernment solutions between the Federal Government, the provinces, and local authorities. The members of the ICT Board were comprised of the Chief Information Officers (CIOs) of the Ministries, who were nominated by their respective ministers. The ICT Board was headed up by the Federal Chief Information Officer, who was nominated by the Federal Government. The Federal CIO coordinated the ideas and strategies that came from the ICT Board with the provinces, municipalities and local authorities. Work groups were formed to provide advice and assistance to ministries as well as to provinces, cities and local authorities whenever the need arose.

Already in this early phase, the ICT Board instituted a mechanism that could be called an eGovernment solution: the exchange of information between the parties is carried out over a dedicated communication platform[2]. This platform is continually being developed and has become one of the most important information sources for the Federal Government, the provinces, municipalities and local authorities. All the recommendations that are cooperated on by the work groups are published on this address in the form of conventions, information, best practices, white papers and use cases. Due to eGovernment's early start in Austria, many of its electronic services and solutions became showcase examples inside the EU, including the Legal Information System[3], the FinanzOnline platform[4], and the land register in the

[2] http://reference.E-Government.gv.at

[3] http://ris.bka.gv.at

[4] https://finanzonline.bmf.gv.at

Justice Department. A historical milestone was achieved with the introduction of the HELP.gv.at[5] platform, which was awarded the eEurope eGovernment Award in July 2003.

The eGovernment Initiative

The "eGovernment Initiative 2003" was started in addition to the ICT Board. The goal of this initiative was to make Austria one of the European leaders in eGovernment and to secure a position in the top five. Austria was able to achieve this goal largely due to the efforts and preparations that had been in the making since 2001. By 2004, Austria had already reached fourth place in EU benchmark tests. By the next year in 2005, Austria had worked its way up to second place, which put it on track to claim the title of European Champion in 2006 and make it one of the showcase countries for eGovernment in the EU. Austria was able to successfully defend its title in 2007, despite stiff competition in a highly dynamic area -- a fact that deserves special recognition, considering that Austria was able to increase its already high percentage ratings over the previous year.

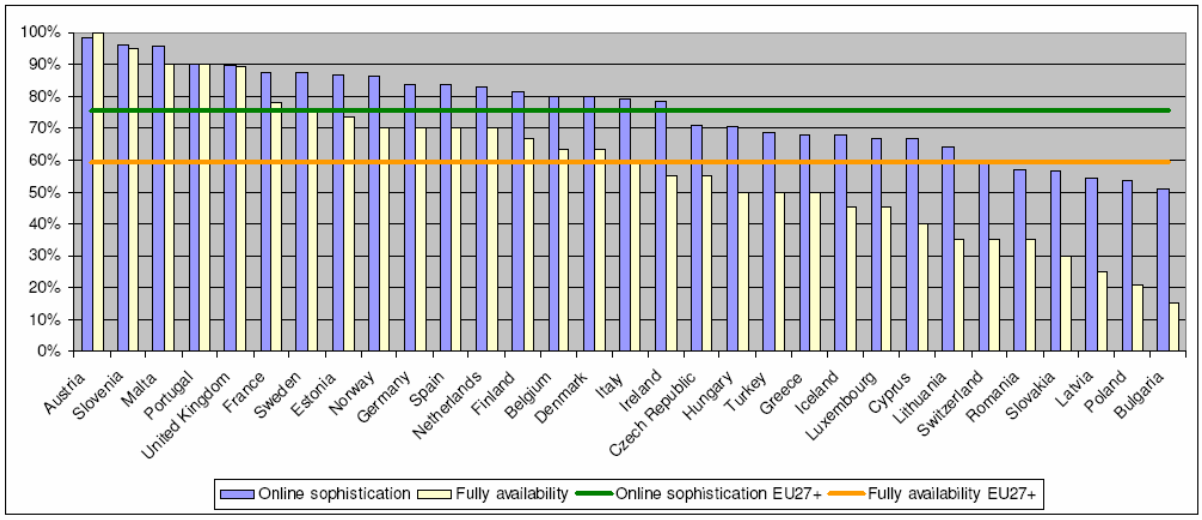


Figure 2: Comparison of online sophistication und availability in EU-wide comparison

The basis for the success was due above all to the ICT strategy adopted in 2001. Austria did not concentrate its efforts on a

[5] http://www.help.gv.at

multitude of short-lived solutions, but rather on building an open and scalable infrastructure that could be expanded on, which at the same time would be secure and sustainable in the long-term. This success story is inspiring enough in itself, but it also demonstrates the need to continuously keep up-to-date, especially in fast moving areas like technology.

eGovernment Platform

An important political impetus behind eGovernment in Austria was the creation of the "eGovernment Platform" under the chairmanship of the Federal Chancellor. The eGovernment Platform handled the overall coordination of eGovernment activities and cooperation efforts were taken over by the newly appointed position “Federal Executive Secretary for eGovernment”. In order to help eGovernment get up and running fast and to realise the goals laid out in the Initiative eEurope 2005, the platform was made available on a wide scale.

The eGovernment Platform was composed of the Vice-Chancellor, the Minister for Justice, the Minister for Home Affairs, the Minister for Finance, the Secretary for the Arts and Media, the trio of chairmen of the Provincial First Ministers’ Conference, the presidents of the municipal and local authorities’ associations, the chief association of social insurance organisations, the Austrian Chamber of Commerce, the Main Association of Austrian Social Security Institutions, the Federal CIO in his capacity as Chairman of the ICT Board, and the directors of the legal and technical eGovernment working groups of the provinces. This list provides an idea of the scope in which this platform was applied in order to exact the maximum amount of effectiveness in implementing innovative eGovernment ideas.

eCooperation Board

The *eCooperation Board* was also created at the same time as the eGovernment Platform. Its function was to support the eGovernment Platform in achieving its goals. The eCooperation Board, which was headed up by the Federal Executive Secretary for eGovernment, was composed of representatives from all ministries provinces, local and municipal associations as well as

other interest groups. As its name implies, the main tasks of this board were to coordinate works in progress, discuss plans for implementation, select project leaders and follow the goals laid out in the eGovernment Roadmap.

The eGovernment Roadmap Up to 2005

Austria's ability to work its way up from the middle of the ranks to the top position in the EU within such a short time was not just due solely on the basis of their ideas, team work and good cooperation. It was due just as much to the fact they had the right strategy and a plan of action, in the form of a roadmap that was followed through on and achieved by 2005. For every project there was a short summary of project information that outlined the goals, priorities, project leadership, project members and project realisation date. The actual implementation of individual projects was carried out by various work groups that were made up of experts chosen from across the country in different provinces, cities and communities as well as those from various business sectors, according to their interests and expertise.

Federal Platform DigitalAustria

The high level of distinction that eGovernment now enjoys in Austria is seen in the fact that the responsibility for the overall coordination of eGovernment been transferred to the Federal Chancellery. The general term for it is the Federal Platform Digital Austria (PDA), which was created in 2005. It has become the centre stage for coordination and strategy of eGovernment in Austria by the Federal Government. All eGovernment projects in Austria now run under the Federal Platform Digital Austria designation. It coordinates all the agendas of the "Cooperation BLSG" (which stands for Federal Government, Provinces, Municipalities and Communities), formerly known as the eCooperation Board, and the Federal ICT Board. The advantages of having a single chairmanship in charge of projects are obvious. Projects are coordinated with one another so any projects which are too similar can be detected and duplication of effort can be avoided. The chairmanship of Platform Digital Austria is held by the Federal CIO.

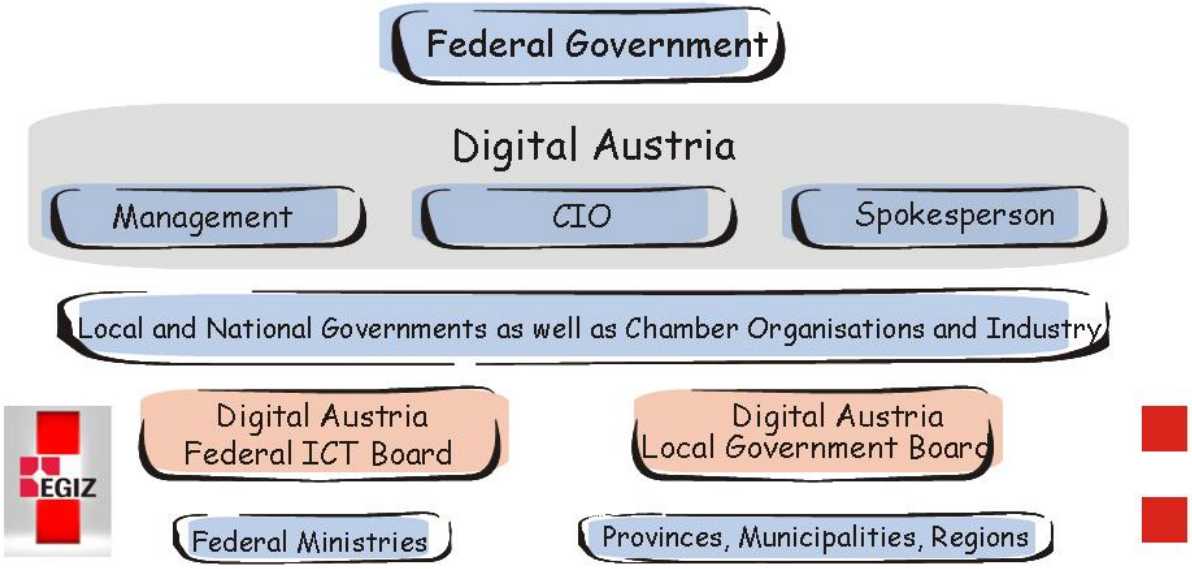


Figure 3: Committees and structure of eGovernment coordination

The eGovernment Innovation Centre (EGIZ[6]) was established at the same time as the platform. The initiative between the Federal Chancellery and the Graz University of Technology supports the Chancellery in the development of an ICT federal strategy and carries out technical research in the field of eGovernment. The main areas of focus of the EGIZ include various topics in IT security, further education and training, strategic and technical consulting for public administration and participating in international collaborative projects. Since 2006, the Federal Platform Digital Austria has been working in close cooperation with the Centre for eGovernment at the Danube University in Krems in the areas of e-democracy and eGovernment education and training.

The Federal Platform Digital Austria's[7] web site serves as the main information source for eGovernment in Austria. It contains comprehensive information on the current goals and focus of eGovernment, tailored to various target audiences.

[6] http://www.egiz.gv.at

[7] http://www.digitales.oesterreich.gv.at

Equipment

What kind of technical infrastructure do citizens and businesses need in order to take advantage of eGovernment? One of the most important requirements in the action plan of the eEurope 2005 is the "eGovernment for all" mandate. In order to reach this goal, there needs to be an adequate IT Infrastructure available in each province. In Austria, this is already the case: 65 percent of households have an Internet connection, 30 percent of which is a broadband connection. Even mobile broadband has become quite popular with 6 percent. Internet access is becoming more and more common. For businesses, a broadband or dedicated connection is regarded as standard.

This technical base is necessary in order for eGovernment to work. Access to electronic government services should be available for every citizen who wants to use it. For all those who do not have an Internet connection either at work or at home should be able to access the services using public terminals, like the Multimedia Stations from Telekom Austria (which have been installed country-wide in Austria as the next generation in telephone booths). Currently there are over 850 Multimedia Stations[8] Austria-wide. To give all Austrian citizens the opportunity to take part in the eGovernment experience, an initiative of the Federal Chancellery in cooperation with Telekom Austria was carried out in 2003 that made it possible for users to view Web sites that end with gv.at on these stations free-of-charge. Even citizens who do not have their own Internet connection can use these terminals to conduct transactions with public authorities electronically.

The improvements being made in eGovernment makes it possible for more and more complex transactions to be offered, for example, those that ask you to confirm your identity or require your personal signature. For transactions that require you to uniquely identify yourself, the citizen card is the method of choice. The Citizen Card chapter covers the various ways that a citizen card can be obtained and describes the technical equipment that is needed for it.

---

[8] http://www.multimediastation.at

Citizens

How Electronic Services Make Life Easier

For citizens, the step by step implementation of eGovernment makes everyday life much easier. The inconvenience of having to carry out business in person at a public administration office will no longer be necessary since the majority of transactions will be carried out online. The wide breadth of services that can be made available can save a lot of time, energy, and inconvenience and eliminate unnecessary formalities. They include anything from applying for online grants to visiting the Web site of the Tax and Revenue Office, requesting a Criminal Record Certificate, or finding out about the textbooks for school children program.

Many types of electronic forms are already available online and more are planned for the future. These forms are available on the Internet and in many cases can be filled out and submitted directly online.

The step into the digital world for public authorities means that in many cases it will no longer be necessary to show up at the public authority in person during specified office hours. Important public authority business can be carried out with a few mouse clicks 24 hours a day, 7 days a week. It eliminates having to spend time in waiting rooms or having to fill out and hand in a paper form in order to request vacation time.

Electronic signature

The “electronic signature” is one of the core components of many eGovernment solutions. The purpose that this component serves can be explained quite easily. Many application forms require the signature from the person filling it out, which until now had to be signed on the paper itself. With the changeover to electronic services, authenticating by signature has to be carried out electronically. There needs to be a method for adding an electronic signature to a document that provides adequate security, yet is still easy enough to use.

An electronic signature is not just a signature on paper that has been scanned in. It is a mathematical operation that is carried out automatically by the sender and recipient using two keys.

Together, these keys form a unique pair. If both keys fit together, the recipient is ensured that the content is really from the person who sent the signature. For electronic signatures, the following aspects are important:

- Authenticity: The message really comes from the given sender and the sender can be uniquely identified.
- Integrity: Manipulation of the signature or the signed document can be detected immediately

In addition to using an electronic signature, the document can also be electronically encrypted. Only the actual recipient of the document will be able to decrypt it and read its content.

Which steps and technical devices are required in order to send documents with an electronic signature from work or home? First of all you will need a computer with an Internet connection and a card reader. The card reader can either be integrated into the computer itself or you can connect an external one to it.

You need a card that has the digital signature certificate saved on its chip. You can even use one of the cards you already have in your wallet, such as your bank card or your social insurance e-card. These cards can be used as "citizen cards" (see following section) for conducting transactions with public authorities over the Internet. The concept of the citizen card does not rely on a particular data storage medium.

The Citizen Card

The citizen card is a necessary tool in many areas of eGovernment. In order for public authorities to be able to identify someone, they need an electronic tool that verifies his or her identity. An Internet portal was created for the citizen card that contains more information on this electronic identification card and how it works[9].

[9] http://www.buergerkarte.at

Figure 4: The citizen card Web site

So how does one obtain a citizen card? A card which gives you access to all public authorities on the Internet? If you have an e-card or a bank card, then you practically have one already. You only need to activate it in order to get started.

- e-card: Most Austrians have a social insurance e-card. To use this card as a citizen card, you only need to visit the Webservice[10] from A-Trust and follow the instructions there.

[10] https://www.A-Trust.at/e-card/

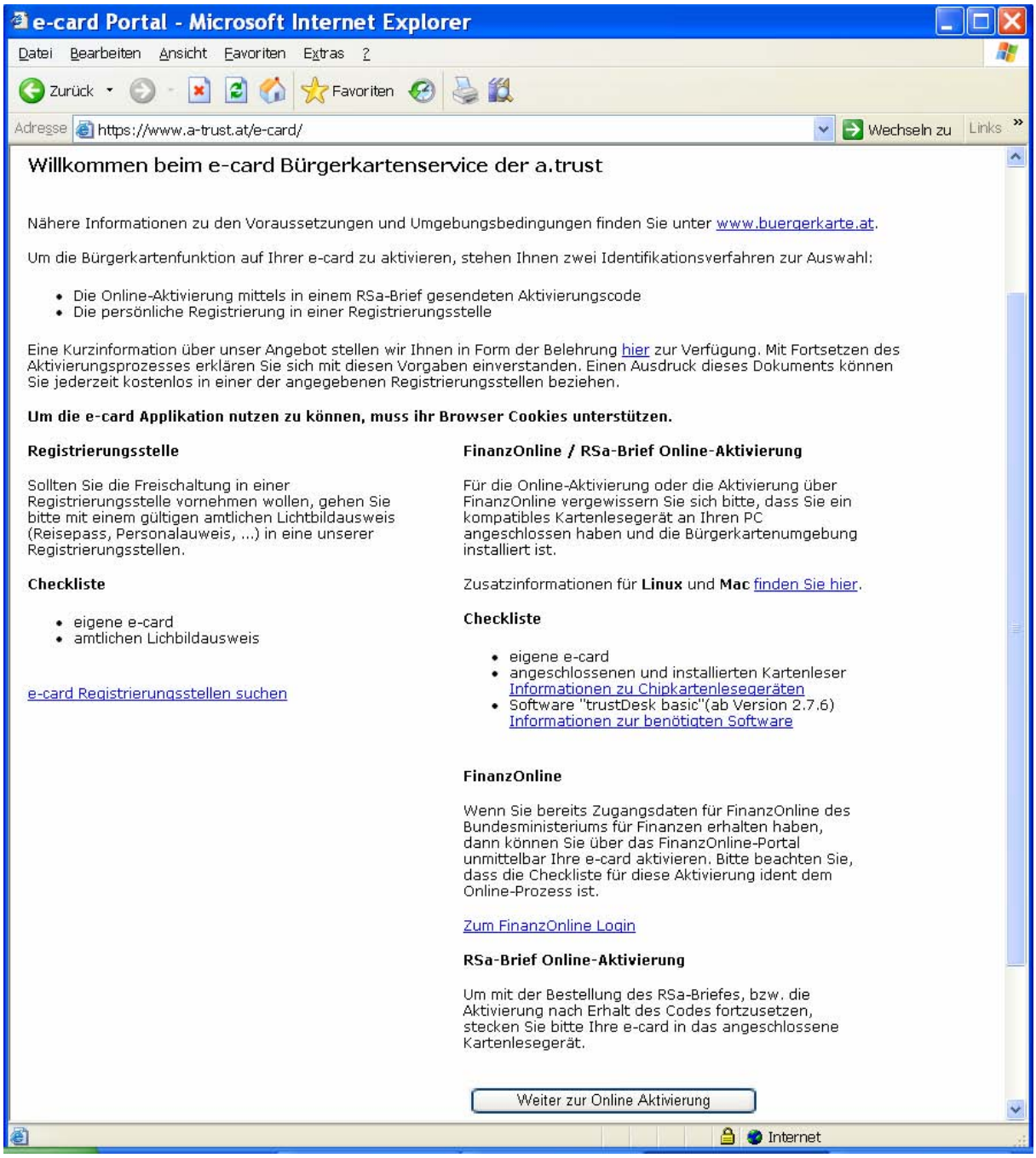


Figure 5: Free activation of the e-card to use as a citizen card

As mentioned in the previous section, you need a PC and a card reader for inserting the e-card. In addition, you also need to download and install the necessary citizen card software, called the Citizen Card Environment. This software is available free for download[11] for all of the most commonly used operating systems. If the citizen card function has been

[11] http://www.buergerkarte.at/BKU/Index.html

activated on your e-card using the Webservice from A-Trust, it can be used as a citizen card immediately afterwards. And the best thing about using the e-card as the citizen card is that the activation and its use is free of charge.

- Maestro bank cards: Your bank card can also be used as a citizen card. You can activate it at different locations, such as in many bank branches. A list of places where you can register your bank card is available on the Internet on the A-Trust[12] Web site. Further information can be found on the Europay[13] homepage. You can find out what the current costs for this service are on the A-Trust site.

[12] http://www.A-Trust.at/registrierung/product_search.asp

[13] http://www.maestro.at/epa/opencms/de/Home/Maestro_verwenden/Digitale_Signatur/

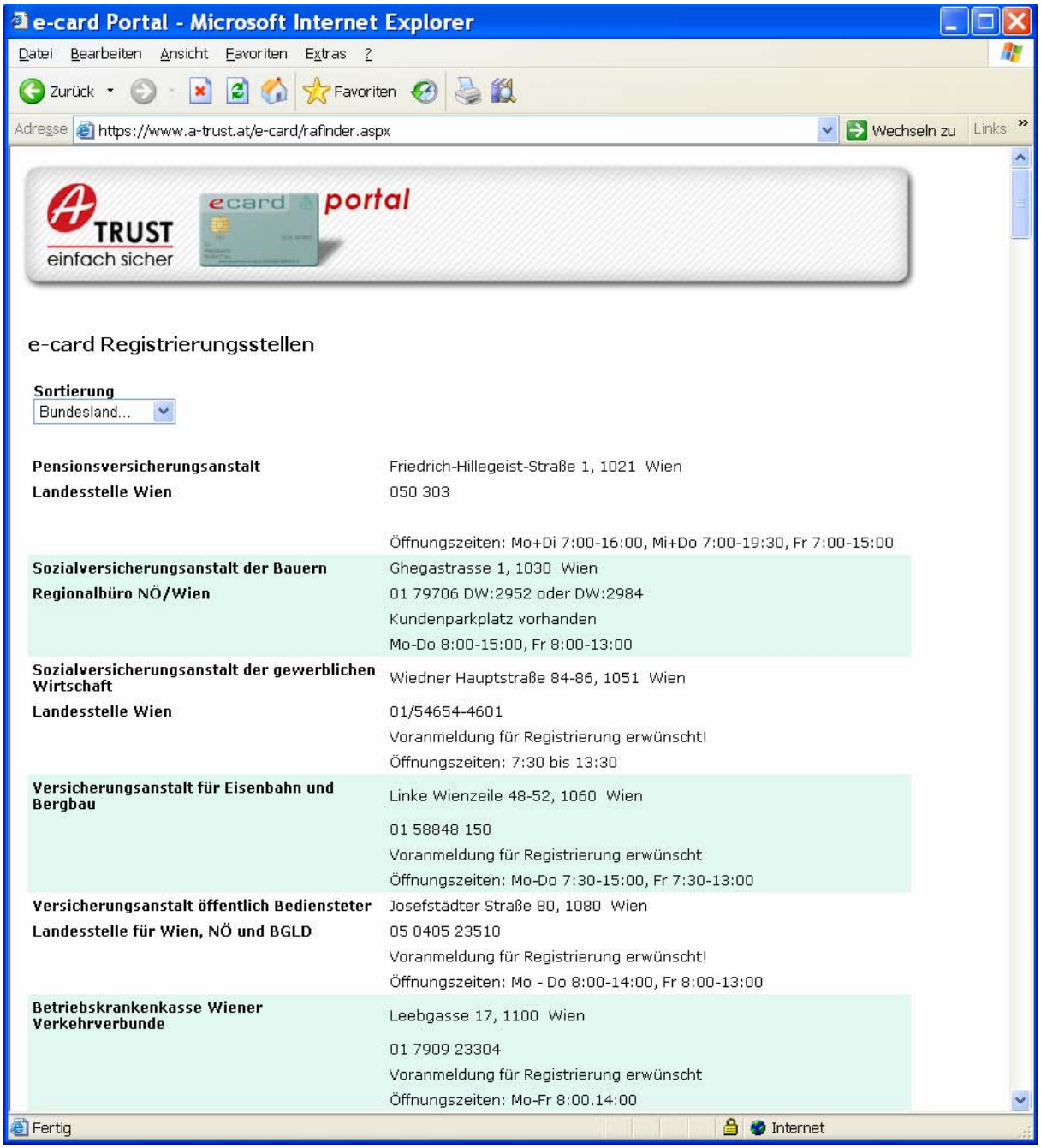


Figure 6: List of registration sites

Electronic Mandates

You can also use the citizen card to conduct transactions on someone else's behalf, provided that the proper authority has been granted. On the "Vollmachtenservice der österreichischen Stammzahlenregisterbehörde" (Electronic Mandate Service of the Austrian sourcePin Register Authority)[14] page of the Austrian Data

[14] https://vollmachten.stammzahlenregister.gv.at/mandates/

Protection Commission Web site, you can apply to save a confirmation of the existence of a mandate on the citizen card.

Electronic Payments

Many public authorities' services have fees attached to them. In order for the transaction to be carried out completely online, there needs to be a way to transfer money electronically. It is possible to pay using a credit card, as is commonly done when items are bought over the Internet. Therefore, a high value is placed on security for all eGovernment pages in order to prevent any possibility of misuse.

Those who do not have credit cards can use an eps online money transfer instead. In order to use this option, you will need to have an online banking account with your bank. Information on online banking can be found on the Web sites of the respective institutions or in your local bank branch[15].

eGovernment Quality Mark

The Austrian eGovernment Quality Mark was created as a result of an initiative of the ICT Board and the Austrian Federal Government in 2003. The Quality Mark is awarded by the Federal Chancellery to eGovernment solutions that prove to be strategy-conform. It is meant as a quick and easy way to inform users of eGovernment Web sites as to the trustworthiness and security of the respective pages, applications and products.

[15] This payment option is currently offered by Raiffeisen-Bank, BA-CA, Erste Bank, BAWAG/P.S.K., Hypo Oberösterreich, Hypo Salzburg, Hypo Steiermark, Hypo Niederösterreich, Hypo Tirol, Hypo Vorarlberg and the Volksbanken.

Figure 7: The eGovernment Quality Mark

The eGovernment Quality Mark ensures users that the Web site adheres to the strict requirements of Austrian eGovernment. Users can conduct business with authorities on the site without hesitation. The latest information on the Quality Mark can be found on the Federal Platform Digital Austria's Web site[16]. The results of the eGovernment cooperation between the federal government, the provinces, municipalities, local authorities and other public organizations are reflected in the Quality Mark, which in turn benefits citizens even further.

The Citizen Card in Practice

New applications are constantly being developed that can be used with the citizen card over the Internet. The most important public authority services are already accessible using the citizen card. A list of all federal[17] and regional applications[18] can be found on the HELP.gv.at platform[19].

The Help Portal HELP.gv.at

The first place to go for questions about public authorities or electronic eGovernment services is the HELP.gv.at portal.

---

[16] http://www.digitales.oesterreich.gv.at/site/5422/Default.aspx

[17] http://www.help.gv.at/sigliste/sig_bund.jsp?cmsid=281

[18] http://www.help.gv.at/sigliste/sig_region.jsp?cmsid=281

[19] http://www.help.gv.at

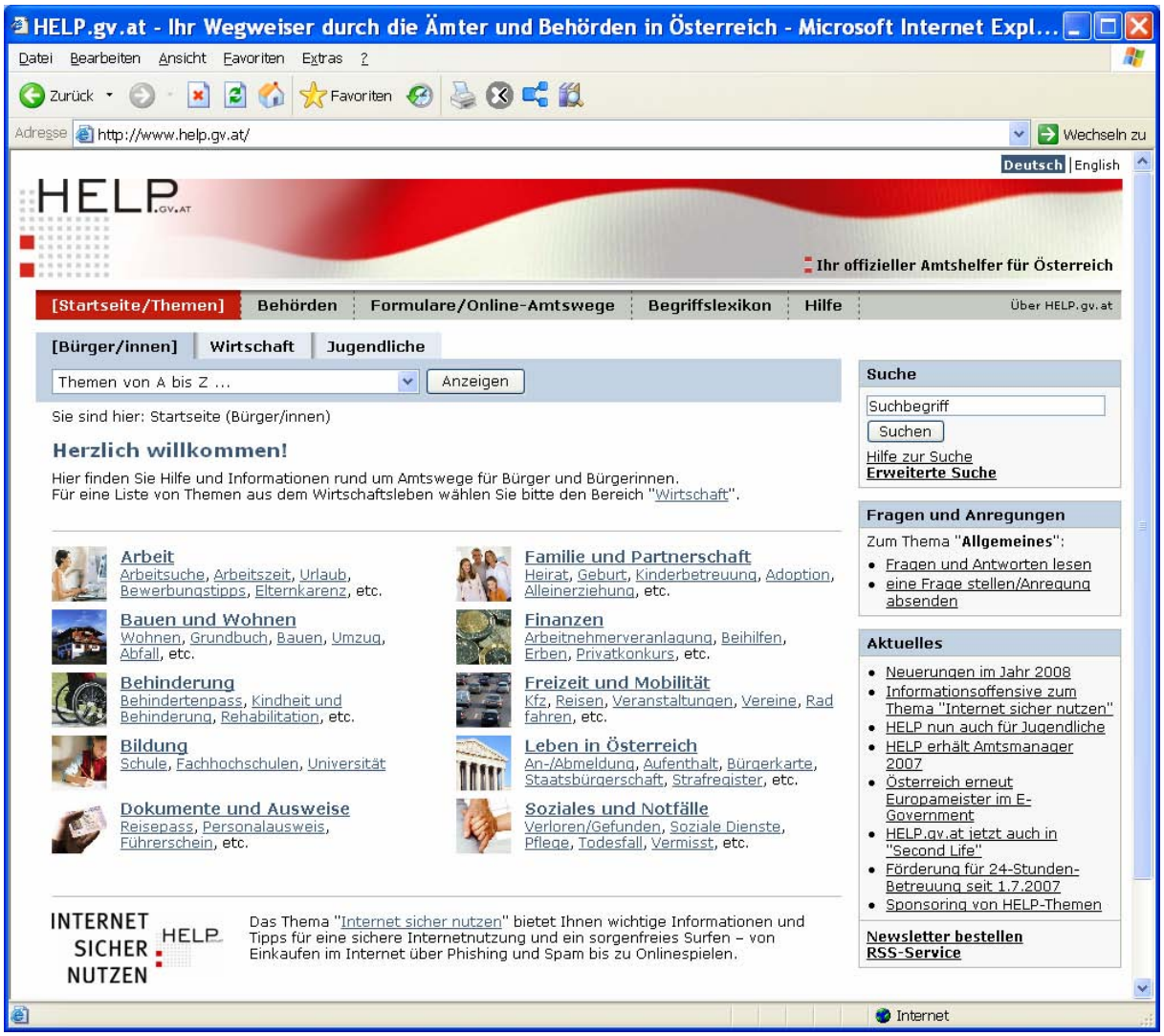


Figure 8: The HELP.gv.at homepage

The Web site is designed to be barrier-free so that it can be used with ease by those with special needs or older people with diminished eyesight. The navigation was designed to be as simple and straightforward as possible so that users do not need to click around too much in order to find the desired area. All available content is listed from A to Z and also arranged according to topic into major categories and themes. Categories such as Education (which includes forms for registering for school), Documents (like the form for applying for a passport), or Finances (where online income tax forms are located) can be found on the HELP.gv.at platform[20]. The HELP.gv.at site also contains general information on

[20] http://www.help.gv.at

eGovernment services and provides links to the corresponding solutions.

The menu item "Formulare/Online-Amtswege" (Forms/Online procedures) contains an exhaustive list of application forms for all public authorities in Austria, from A to Z. The application forms found here can be downloaded, filled out and sent to the corresponding authority by regular post or e-mail. Many of the application forms can even be filled out and signed directly online, entirely paperless and without any further action necessary.

FinanzOnline

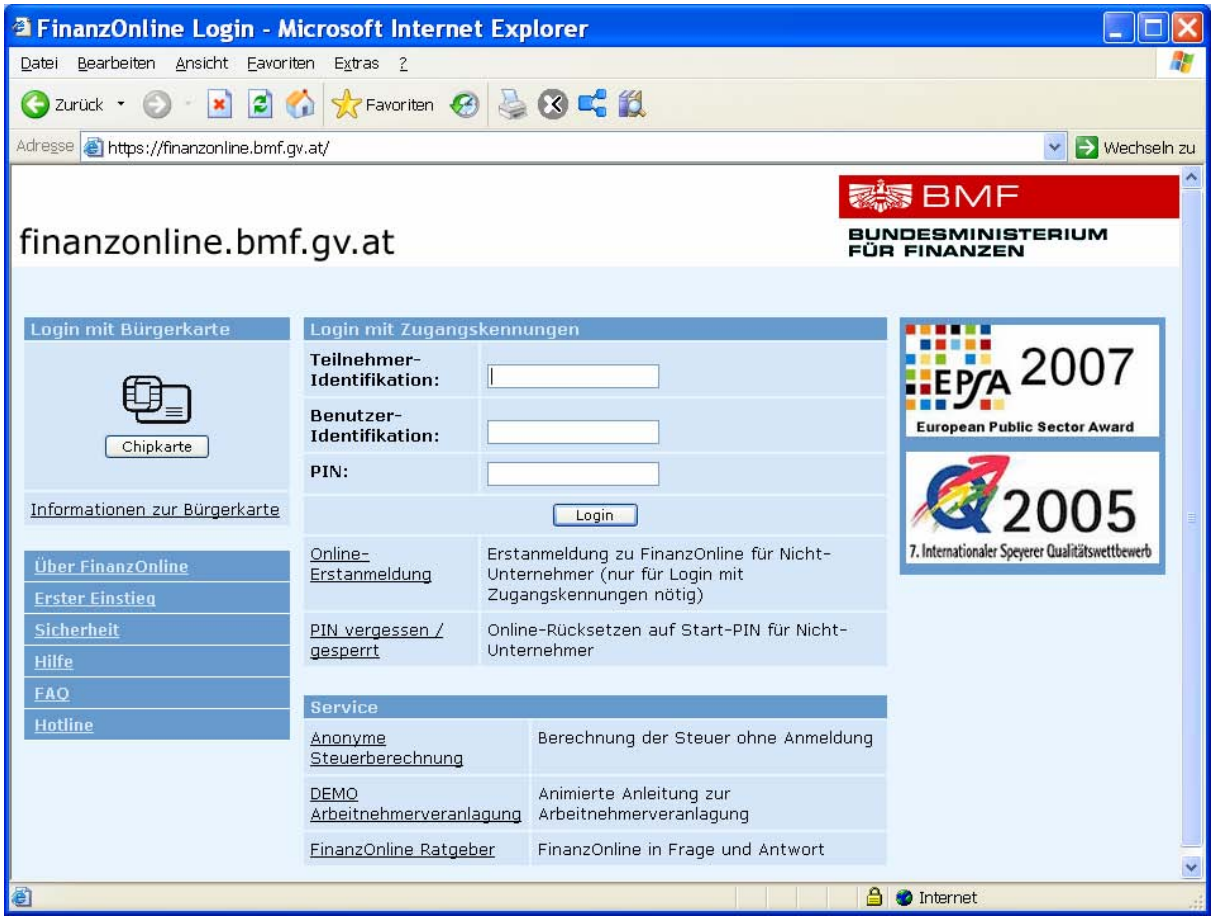


Figure 9: FinanzOnline homepage

On the FinanzOnline[21] site, anyone aged 16 and above can fill out an income tax form online. To use the citizen card, you must already have the Citizen Card Environment software installed on

[21] https://finanzonline.bmf.gv.at

your computer. Then you only need to insert your card into the card reader, click “Chip card” and confirm the “Accept this certificate” message that appears. After you enter your pin code, you will be taken to the homepage which shows an overview of the most important information.

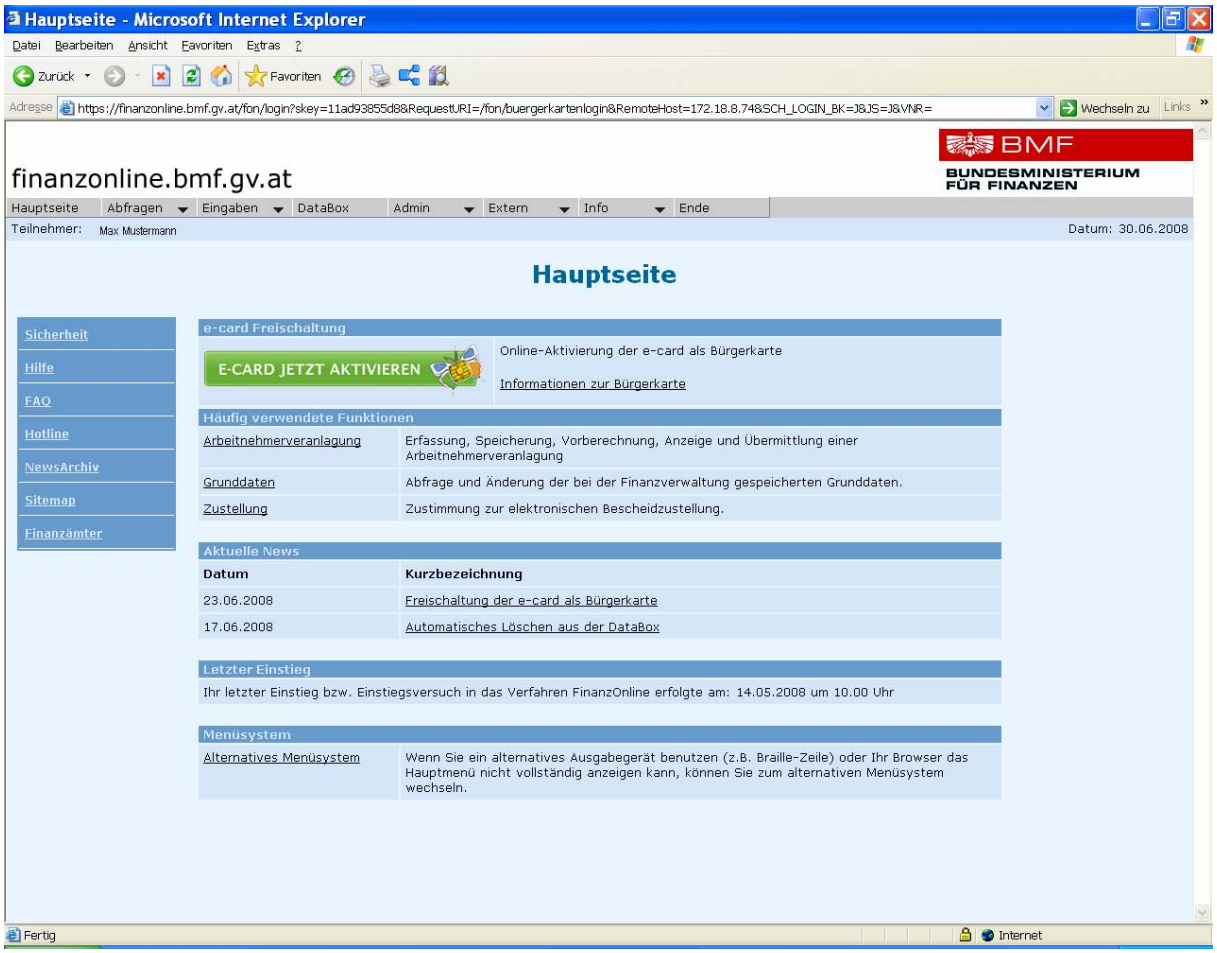


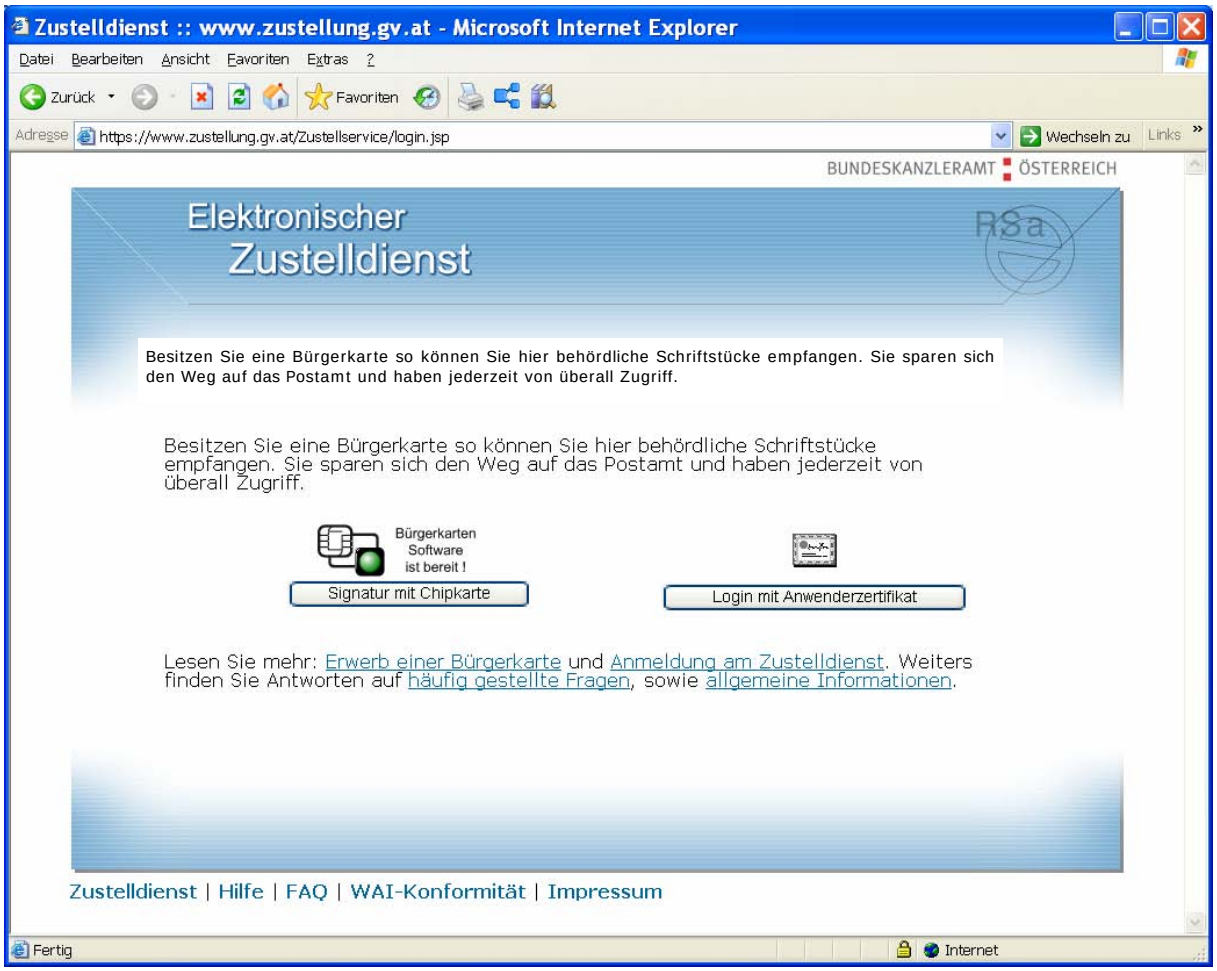
Figure 10: The FinanzOnline homepage after successfully logging in

Navigate to the desired area, for example, to the income tax form page, and enter your information in the form provided. All communication between your computer and the finance office is encrypted so that no one will be able to access and read the document after it has been filled out. After you are finished filling out the form, the data is sent to the finance office.

The user has the possiblity to acticate his/her citizen card after providing his/her identification via username/password.

Electronic Delivery

Official notifications and correspondence, such as RSa and RSb letters, are sent in most cases via regular post. If the addressee is not currently present when the letter arrives, he or she will have to go to the postal office in person to pick up the letter after showing proper identification. With electronic delivery, this inconvenient and time-consuming procedure is no longer necessary. It only takes a one-time registration (free-of-charge, of course) of your citizen card at an electronic delivery service[22] and you will be able to download official notifications and correspondence over the Internet. However, it is important to check whether the electronic delivery is supported by the particular public authority. When a new piece of correspondence arrives, you will be notified, for example by e-mail.



[22] E.g.: https://www.zustellung.gv.at

Figure 11: Homepage of an electronic delivery service

The following steps are required to pick up official notifications or correspondence:

1. Go to the start page of the delivery service you are registered with and login using your citizen card.

2. If login is successful, you will be able to access your Inbox. The notifications and documents can be printed, downloaded or forwarded.

Figure 12: A document in the Inbox

The two applications that were introduced serve as examples of how the citizen card and eGovernment can eliminate many of the formalities when dealing with public authorities. In the following sections, useful Internet sites and additional electronic services that are already able to be used by citizens will be introduced.

Proof of Residence Form

The document known as the "Proof of Residence form" (Meldezettel) is still important for carrying out many transactions today. The form to apply for a Proof of Residence document can be obtained at the local municipal authority direct, or downloaded from the Internet.

In order to apply for the form over the Internet, you must have already registered at an electronic delivery service (see above) so that the municipal authority is able to send it over the Internet. The application itself has a remarkably simple design. The online application form for the Proof of Residence [23] document is available on the HELP.gv.at platform.

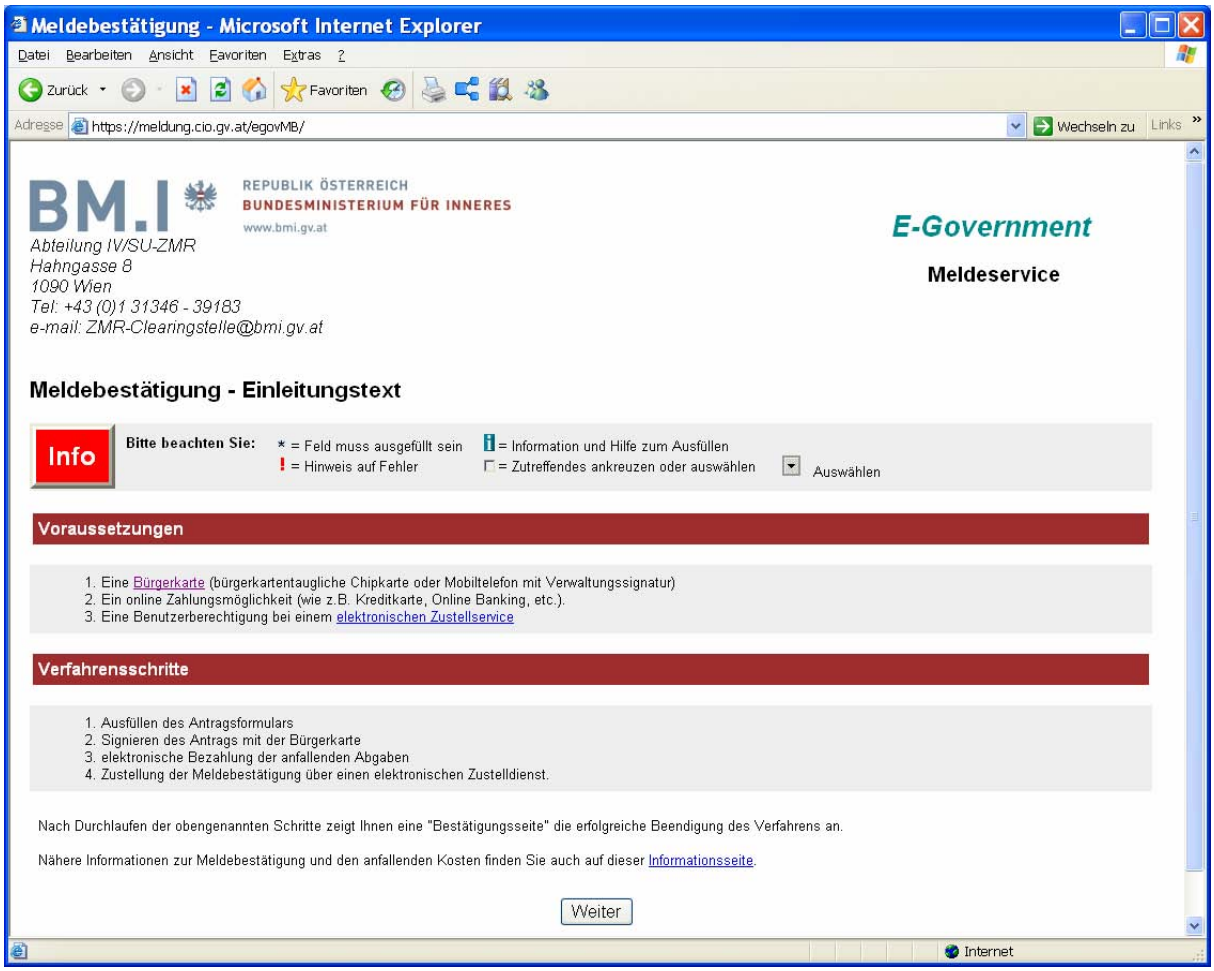


Figure 13: Application form for Proof of Residence

[23] http://help.gv.at/linkhelp/besucher/db/formularauswahl.formular?id=562

The application form must be filled out and electronically signed using the citizen card. The fee can be paid using an online payment service. Your residence registration document is delivered shortly thereafter to your inbox.

Criminal Record Certificate

A Criminal Record Certificate certificate can be applied for just as easily. In the past, this document was also referred to as the “certificate of good conduct”. It contains information about any convictions that were entered into the register, or states that no entries were found if the person has a clean record. Providing an up-to-date certificate that shows a clean record is a requirement for many jobs and occupations (for example, for obtaining a business licence, or being hired by a security guard company). In most cases, the certificate needs to be less than three months old.

Bundespolizeidirektion Wien
Strafregisteramt

Wasagasse 22 — Gebühr entrichtet
1090 Wien

BEZUG: SB INTERNET SRB2008072509213901
(REFERENCE NUMBER)

STRAFREGISTERBESCHEINIGUNG
(CRIMINAL RECORD CERTIFICATE)

Familienname(n): Mustermann
(Family Name)

Geschlecht: männlich
(Gender: MALE)

Vorname(n): Wendelin
(First Name)

Akad. Grad: Dr.
(Academic Degree)

Geboren am: 29.02.1956
(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: 09.40.08
(Time)

REPUBLIK ÖSTERREICH BPD AMTSSIGNIERT	Verfahren	urn:publicid:gv.at:form+srb-1.1
	Datum	2008-07-25T07:40:08
	Aussteller	CN=a-sign-corporate-light-02,OU=a-sign-corporate-light-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Seriennummer	82210
	Signaturwert	K2cnpsv3hJZ0jwbQLTsckncwSD+afqIn1XhzqYiy3Z3xnN+jrgnBpsZODs w3/5e8t7ytTUMzkvVptjitLOT4b09n6/F3xWEA+DK0q/0nrOFfV6Fvxzyj l6KXh9WyvJ6JXKMntl0a4cqQlyMYrURMt0uQA5i7aIQ9MNZ2+wz7db8=
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://apps.egiz.gv.at/srb-ver2	
Hinweis	Dieses Dokument wurde amtssigniert. Auch ein Ausdruck dieses Dokuments hat gemäß §20 E-Government-Gesetz die Beweiskraft einer öffentlichen Urkunde.	

Figure 14: Criminal Record Certificate

The Federal Police Headquarters in Vienna offers a Criminal Record Certificate[24]. The steps for obtaining the certificate are similar to those for the Residence Registration document, including using an electronic delivery service and paying fees using an online payment service (e.g., via online banking or a credit card).

eGrants

Some students at Austrian universities and colleges are reliant on financial aid. It was important, in this area especially, to remove the most major bureaucratic hurdles through the introduction of eGovernment applications to make it easier for students to gain access to financial support.

The Student Support Act requires a plethora of evidence and proof from the applicant, which has to be processed by the corresponding authority and must be presented again each time that the grant is renewed. The online application procedure[25] has drastically reduced the time and effort involved. After the application is sent, the system automatically checks once a year whether or not the applicant is eligible based on the available data. It then creates both the application and confirmation forms, likewise automatically, for renewing the grant. The only other thing the student needs to have, other than fulfilling the eligibility criteria, is a citizen card for submitting the application form.

Additional eGovernment Services

The Austrian government offers many other Internet applications in addition to those for the citizen card that can be used by all citizens. The wide breadth of services encompasses a variety of areas, from information about laws and regulations to employment agencies, databases with all brochures from the state.

---

[24] http://help.gv.at/linkhelp/besucher/db/formularauswahl.formular?id=600

[25] http://www.stipendium.at (Menu item „Antrag“)

RIS – The Legal Information System of Austria

It is one of the oldest public government projects in the Internet: the "Legal Information System"[26] (Rechtsinformationssytem) has been in existence since 1997. This database can be used not only by law students and lawyers, but by all citizens to look up current and historical laws.

The Legal Information System (RIS) is operated by the Austrian Federal Chancellery and is used, above all, to announce legislation which must be declared by law in the Federal Law Gazette (BGBl) and to provide information about laws of the Republic of Austria. While developing the system, requests from citizens, interest groups, businesses (e.g., those in the law branch, such as lawyers or public notaries), and those in government were taken into particular consideration.

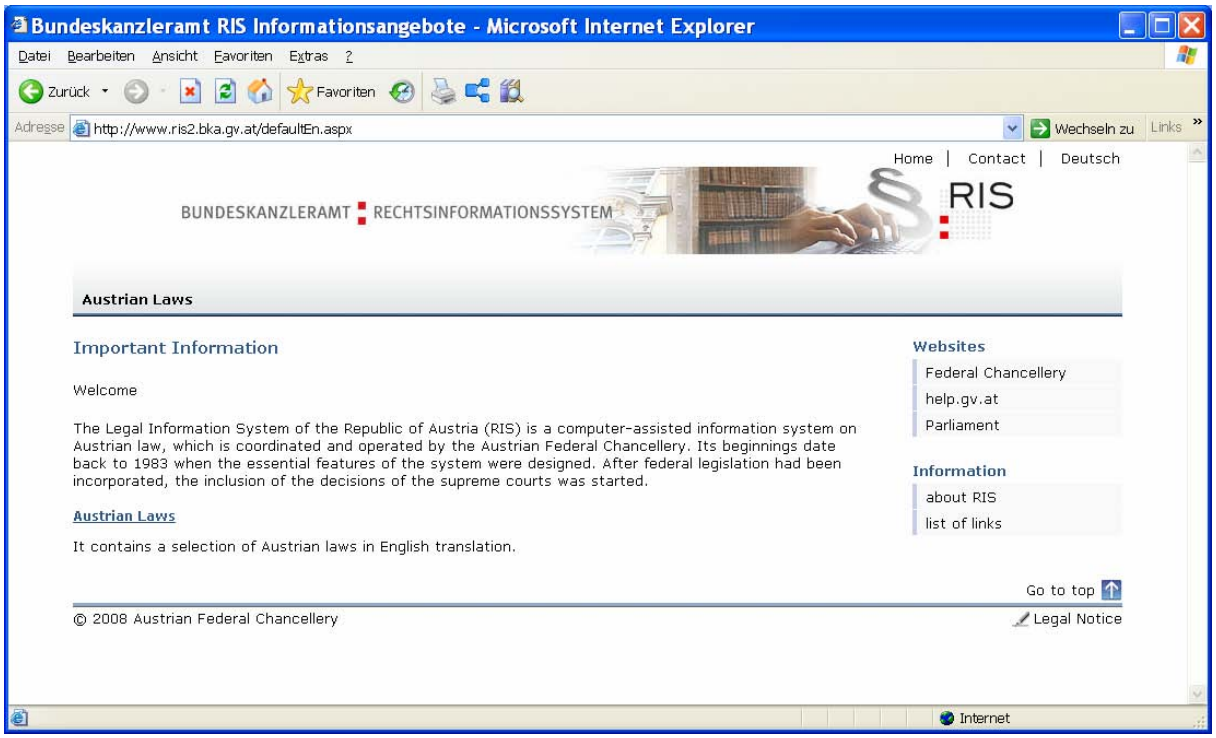


Figure 15: The Legal Information System homepage

[26] http://www.ris.bka.gv.at

The search interface complies with accessibility standards and is very user-friendly. It only takes a few seconds for the search to return the laws that correspond to the given search term. Since 2004, the Federal Law Gazettes must be published by law in the Legal Information System.

The electronic signature again comes into play here. In order to ensure the authenticity and integrity of the content, all published laws and legislation are affixed with an electronic signature.

Along with the federal law gazettes, the RIS also contains European community law, provincial law gazettes, and all provincial laws currently in effect. Decisions of all the high courts (the Supreme Court, Constitutional Court, Superior Administrative Court) and further commissions and tribunals are also found there. Selected decrees from the Federal Minister round out the offering. The scope of the Legal Information System is constantly being expanded, including historical laws.

AMS Next Job

One successful eGovernment service has crossed over into a totally different sector. The project "AMS Next Job" helps people who have been given notice or have left their job to find a new position as quickly and with as little paperwork as possible. As part of the labour market reform bill, the development of this new service was taken on by the Labour Market Service (Arbeitsmarktservice, or AMS), which would allow citizens to declare their unemployment status in advance and apply for unemployment benefits, as well as cancel them again over the Internet.

The new idea: by signing up early for the job search, even prior to being unemployed, the chances of quickly finding a new suitable position are increased and the amount of time spent unemployed is minimized. Optimally, unemployment can be avoided altogether if a new job can be found early enough.

For those who want to fill out the forms themselves, the "Meldung zur Stellensuche" (application to search for positions), "Online-Antrag auf Leistungen aus der Arbeitslosen-Versicherung" (online form to apply for unemployment benefits) and "Check-Out –

Abmeldung von Bezug und Arbeitsuche" (cancelling unemployment) are available on the AMS[27] Web site.

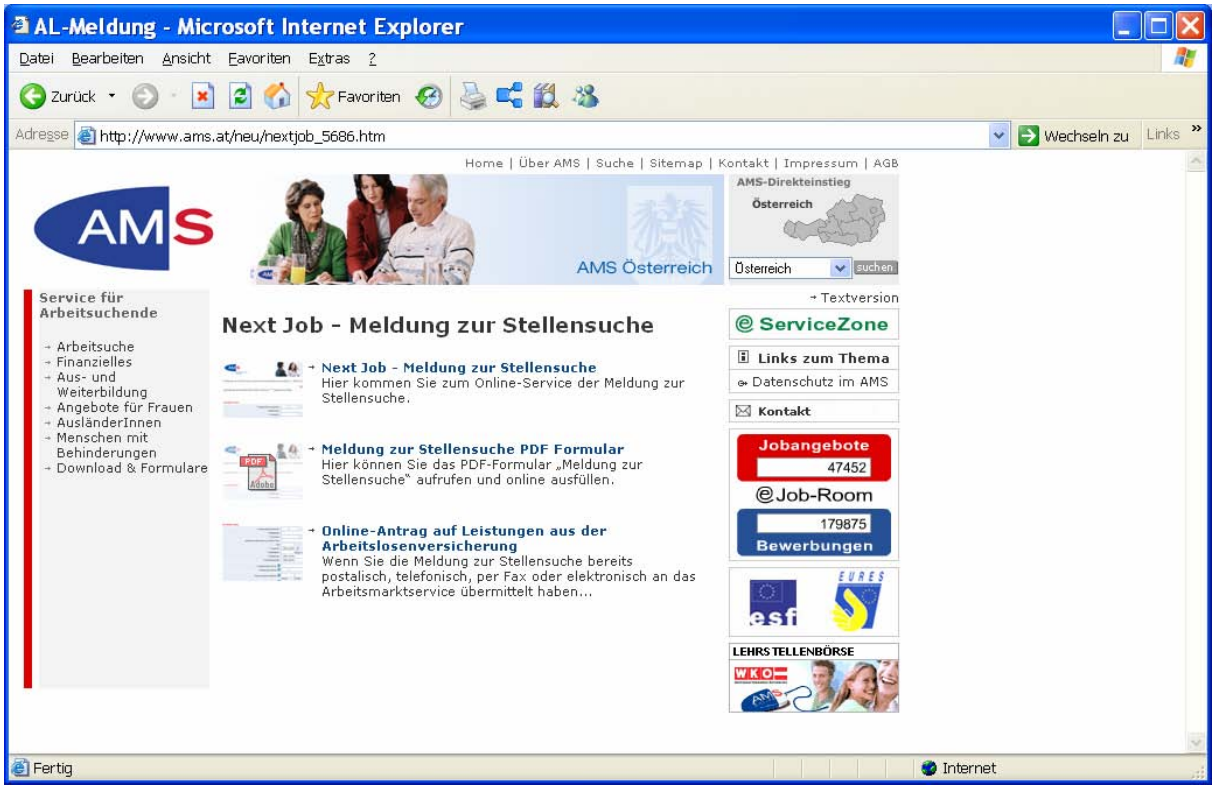


Figure 16: The AMS Next Job Service for people looking for new positions

With "AMS Next Job", customer service was improved, and the amount of time and administration efforts for advisors was reduced. However, its biggest success was to substantially reduce the length of time people spent being unemployed by allowing them to declare unemployment status and search for jobs in advance.

Brochure Database

In addition to the extensive information already available on the Internet, public authorities continue to offer a multitude of brochures on diverse topics. The Federal Ministry for Social Security,

[27] http://www.ams.at/nextjob

Generation and Consumer Protection provides a wealth of publications, in particular on such topics as pension plans, social security laws, planning for elder care and living with disabilities.

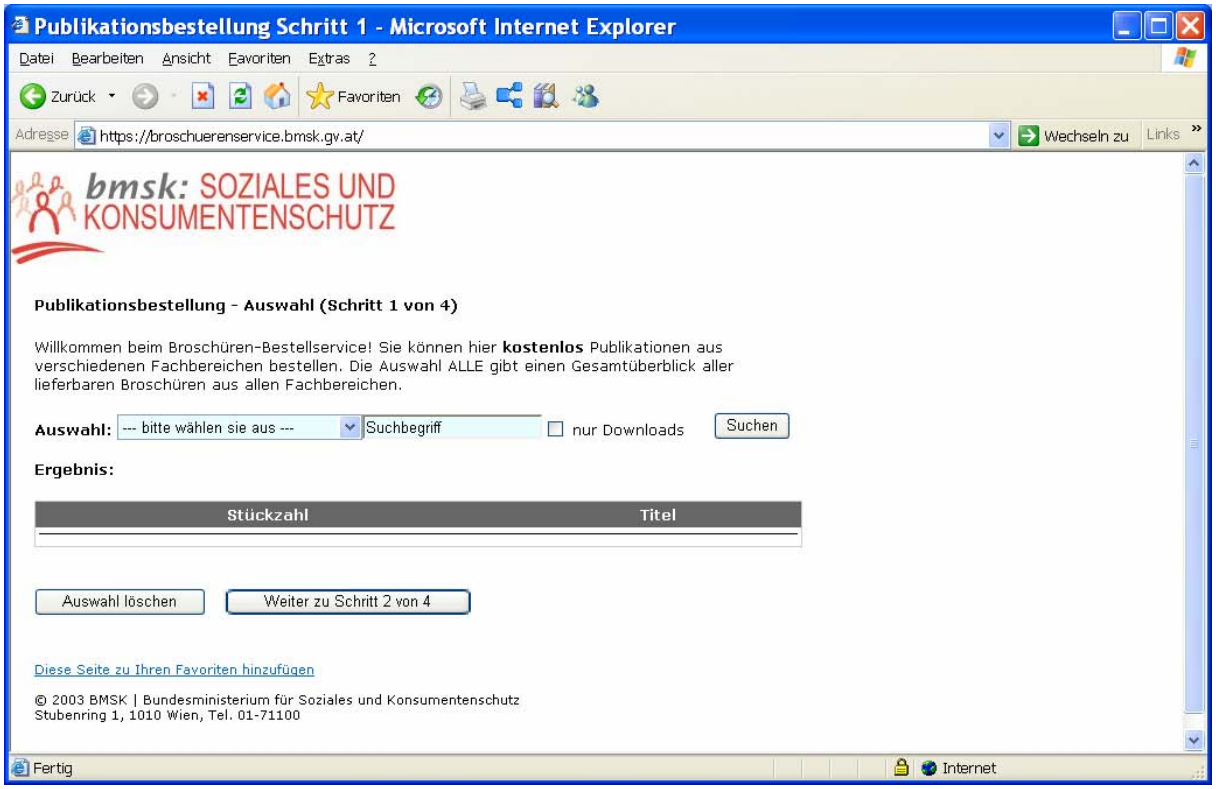


Figure 17: Online publication ordering service

On average, 35,000 citizens a year contact department employees via telephone, Internet and e-mail. Over 350,000 publications are sent out worldwide every year. The goal of the eService of the Brochure Database (BDB)[28] is to manage the enormous administration effort in an efficient manner. Since November 2004, this application has been used to manage all orders, supply stock, and brochure shipments.

These examples contain a large number of best practice cases. A full description of them would go far beyond the scope of this document. All examples are available on the Platform Digital Austria[29]. Anyone having a look is sure to find useful information and answers to any questions they may have.

---

[28] http://broschuerenservice.bmsg.gv.at

[29] http://www.digitales.oesterreich.gv.at

eGovernment Services for Austrian Social Security

Austrian Social Security offers services[30] for people who are insured, contract partners, employers and pharmaceutical companies.

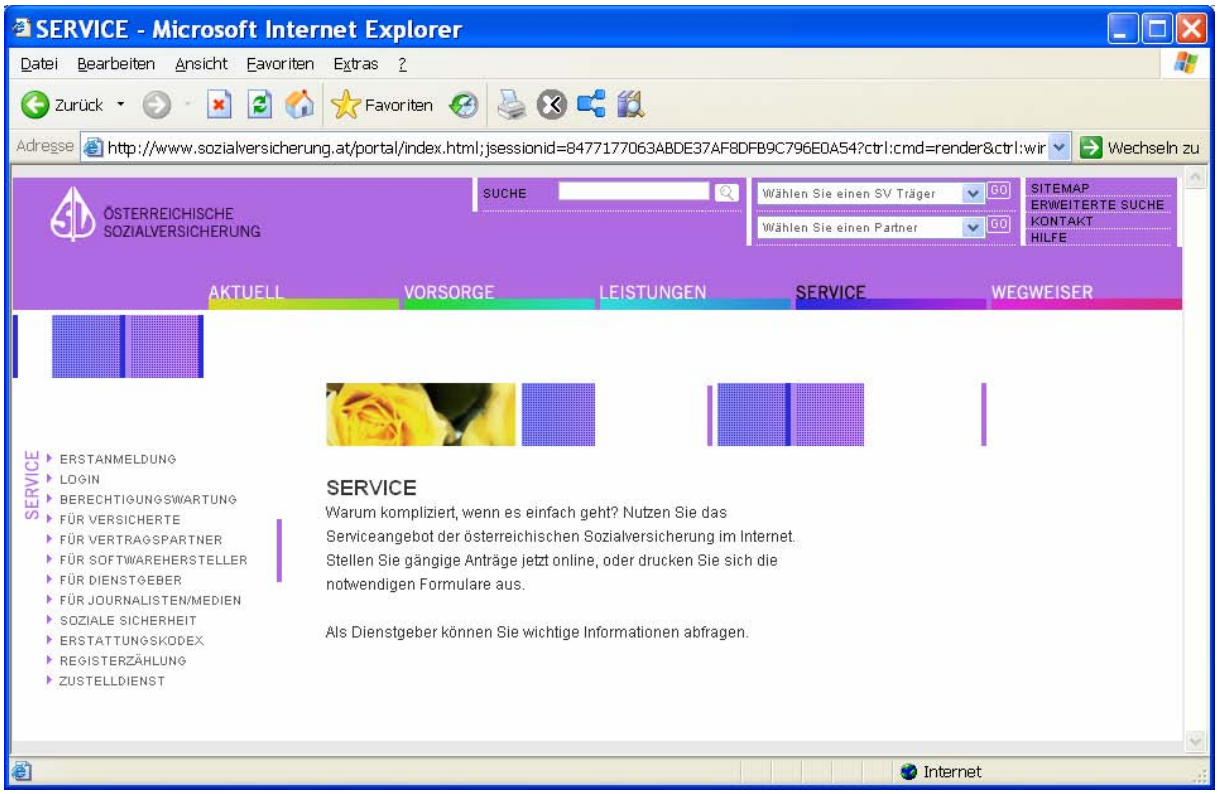


Figure 18: Online services for Austrian social security

For those who are insured:

- Forms (e.g., retirement forms, application for child care allowances, etc.)
- Health insurance data: This service accesses the data stored by the association for social insurance for a given social security number and calculates the amount of services that have been utilised by the insured or his family (up to the date of the application) based on the period insured.
- Health services statement (LIVE): You can look up and print your personal statement of health services that you have utilised.

[30] http://www.sozialversicherung.at

- Personal Retirement Account (ePK): For all men and women born after 1 January 1955 who have retirement insurance coverage have a retirement account reserved for them which contains information on all the contributions from the insured periods.

- Social insurance data sheet (Versicherungsdatenauszug or VDA): The social insurance data sheet contains information on the periods of time that the citizen was insured as well as information on the amount and origin of contributions that have been made so far.

For Contract Partners:

- Pharmaceuticals Authorisation Service (Arzneimittel Bewilligungs Service, or ABS): This regulation along with Reimbursement Code stipulated the requirements that medications can be provided without a prescription, but only on the condition that in place of advance approval, a check-up must be carried out afterwards by the chief physician service of the social insurance organisation.

- Electronic Medical Statement (Befundblatt): The medical statement is filled-out electronically and sent to the social insurance organisation so that the treatment costs can be reimbursed.

- Health insurance data: This service accesses the data stored by the association for social insurance for a given social security number and calculates the amount of services that have been utilised by the insured or his family (up to the date of the application) based on the period insured.

- Contract partner account statement online (VPA online): This is a free service of social insurance for contract partners that allows data to be exchanged securely using the citizen card. It is also used to make an electronic account statement available online to contract partners for whom buying commercial software would not be worth the cost or effort.

- Compensation form (Verrechnungsschein): Contract partners and service providers use this form to send the bill of services to the social insurance organisation.

For Employers:

- Employer account queries: (DG-Net): This service gives employers read access to their account.

Pharmaceutical companies:

- Electronic workflow of the Reimbursement Code (ewEKO): This online service makes it possible for eligible companies to electronically submit application forms for admissions and changes to the reimbursement code.

Businesses

The Essential Source for Businesses

The help site HELP.gv.at is not only an essential information source for citizens, it is also a gateway to eGovernment for businesses. The HELP.gv.at site offers a good overview of the Austrian government, and all information relevant to businesses. The portal contains information and hintfull tips on more than 200 topics and has a comprehensive list of public authorities and forms that can be downloaded from the site. Many transactions with public authorities can be performed online.

In the "Wirtschaft" (Business) section you find information on the public authorities that specifically deal with business and the economy, many transactions can be carried out online - HELP.gv.at is the perfect platform for both employers and employees on the Web.

The business section of the HELP.gv.at site is arranged into six categories, in which business-relevant information on the respective topic can be found. They are "Außenwirtschaft" (Foreign trade), "Finanzen" (Finances), "Hilfreiche Informationen" (Helpful information), "Laufender Betrieb" (Ongoing business), "Mitarbeiter/innen" (Employees) and "Unternehmensgründung" (Starting a company).

For anyone who needs to get a visa for a business partner from another country would find the necessary information in the Foreign trade section. You will find not only comprehensive information on the topic in this section but also the required application forms.

For those with questions about municipal taxes, either on the tax assessment base or on calculating taxes, or for those who want to find out about available grants, they will find the answers in the Finances section.

If a young entrepreneur wants to know which insurance policies are necessary to have or what he needs to do for an environmental impact assessment, he'll find this information in the Business section on HELP.gv.at.

One section that is of interest for both - employees and employers - is found in the Employees menu item on the Portal. This section

contains all employee-relevant information, such as how to register employees for social insurance, info on continuing education and training, and questions about vacation time.

Electronic Transactions

Businesses can decide for themselves whether or not and to what extent they want to carry out transactions with public authorities online. As always, the option to show up in person at the public authority office is open to everyone.

Online services are much easier to use than it is expected. Just as online public authority services are becoming of interest to more and more citizens, businesses are also taking advantage of them more often. A large number of transactions can be carried out from the office with ease, without having to worry about opening hours or having to wait in a long waiting line.

The online procedures build the basis of electronic services for public authorities, which makes life for businesses much simpler. You only need to go to the Internet, for example to the HELP.gv.at site and click on the "Wirtschaft" (Business) menu. From there, forms can be filled-out online and sent directly to the responsible public authority. The forms can be signed using the citizen card, as described in the Citizens chapter, and all applicable fees and costs can be paid electronically. The electronic file is processed by the public authority using the internal ELAK (Worklflow) system. The portal group for local authorities ensures that forms can be processed more quickly. Application forms that are approved are delivered afterwards electronically.

The Citizen Card for Businesses

The citizen card is the main component of performing electronic services between public authorities and businesses. It is used for uniquely identifying users and establishes secure communication towards public authorities.

With FinanzOnline, it is possible to file sales tax, income tax and corporate tax returns online. Electronic tenders save businesses money since it is no longer necessary to produce multiple copies

of the tender documents. Employees can put their citizen card to use at work, if they have an electronic mandate stored on it (see the chapter Electronic Mandate). This allows employees to conduct transactions with public authorities on behalf of the business.

The citizen card is part of the security framework and is available for citizens as well as for consumers. Businesses can offer their own online services and ensure that communication with their customers is secure by making use of the security-relevant functions on the citizen card.

The citizen card has several advantages compared to other systems. The standard username/password system has a high uncertainty factor due to poorly chosen passwords. Research has shown that many computer users choose simple, easy to hack passwords (such as using their own first or last name) or write them even down. In addition to this, passwords can be intercepted over the Internet. All these situations result in unauthorized access. With the citizen card documents and orders can be signed easily and securely. The "digital signature" also offers legal security.

Electronic Payments

Just like traditional transactions with public authorities, fees and charges may also be required for their electronic counterpart. Therefore a way to pay for these costs must be made available online. Many online payment systems are already available today, such as online banking, mobile payment systems like Paybox as well as credit card payment. All of these systems can be integrated into the public authority service. A special interface specifically designed for integrating online payment systems has been already developed, called EPS online[31].

Electronic payments for eGovernment services can be carried out just as fast and easy as in many shops on the Internet today. While the transaction is in progress, the public authority receives an electronically signed message with the confirmation that the

[31] Details in Infrastructure chapter

payment will be received, usually from the bank. The authority doesn't have to wait to complete a transaction, as in the days of the paper payment slip. Instead, the entire procedure can be carried out right away. If "EPS online transfer" is selected as the payment type in an online form, the online banking page of the business' bank will be displayed.

There are many real-life examples of electronic payments being used in eGovernment, such as with the Criminal Record Certificate or the electronic Residence Registration form. After applying to register a residence, the respective fee must be paid using an electronic payment system. Shortly afterwards, the electronic Residence Registration form is sent via an electronic delivery service.

Free eGovernment - the Open Source Building Blocks

Citizen card concept and electronic delivery are implemented in the form of building blocks. In order for eGovernment to be accepted and used by the private sector, open source building blocks are available which can be used by businesses. The term open source means that the source code for a piece of software is open to the public and may be further developed and distributed.

For businesses that are interested in propagating the use of citizen cards, whether e-cards or bank cards, can integrate applications into their systems with help of these building blocks. This not only serves to increase eGovernment's popularity, it also allows businesses to develop their own trend-setting services.

With the use of the building blocks, also known as MOA (Modules for Online Applications), applications can be made more ser-orientedly. They are available on an own open source platform[32]. When citizens sign their online application forms, the MOA on the public authority's or business' page is able to verify the signature. When an authority sends an official notification or a piece of

[32] http://www.egovlabs.gv.at

correspondence, it will be signed with help from the MOA and delivered electronically in RSa letter quality. Even in the private sector it can be used in many different ways, from providing login access using the citizen card to signing official contracts or even sending contracts electronically using an electronic delivery service.

The following MOAs currently exist:

- The server signature MOA SS is used for creating electronic signatures. This allows documents such as notifications or invoices to be signed in batch format, so that they are protected from manipulation.
- Signature verification is carried out by the MOA SP. This module helps not only with the verification of electronic signatures, but also in checking a document's point of origin and its authenticity. Documents that are forged or which have been tampered with are recognized immediately by the MOA SP.
- The MOA ID is used for identification purposes. This module enables secure login via the citizen card as it is already offered for example by "FinanzOnline" and the main association for social security.
- The delivery module, MOA ZS, is responsible for secure delivering documents electronically. Using this module, documents of any kind can be delivered in RSa letter quality to recipients by electronic means.
- MOA AS offers a simple Web service that allows PDF documents to be affixed with an official (electronic) signature by the authority.

eProcurement

With eGovernment it is also possible to purchase goods and services over the Internet. This is referred to as eProcurement. Businesses use it mainly for commercial purchasing. For example, governmental purchasing is beeing taken care of by the Bundesbeschaffung GmbH. This organisation uses the

eProcurement System and opened an e-shop[33] in January 2006. Catalogues from more than 300 suppliers are listed in a uniform system on the portal. Public authorities can order anything here from pencils to laboratory equipment and office furniture over the Internet.

The eProcurement system includes suppliers in the workflow process, which takes small and middle sized businesses into consideration. Businesses that do not have an electronic inventory system can import their product lists in simple Excel format into the e-shop. They are notified by e-mail when a product is ordered. The business then can confirm the order in the Web portal for suppliers. Small businesses in particular gain valuable know-how about electronic business processes. Suppliers with electronic inventory systems can synchronize their data automatically with the e-shop. This workflow process assures businesses that all orders are legitimate.

Regional, small and middle-sized businesses are assisted by the regional filter. For example, a businessman from Tyrol can see in "his" eShop all products from local suppliers in his area. Postal codes are used as a filter criteria.

eGovernment Quality Mark for Businesses

The eGovernment Quality Mark is a signal for businesses and citizens that the respective eGovernment Web site, application/solution or product is trustworthy and secure as well as acting conform to the eGovernment strategy.

Businesses that offer their own eGovernment solutions can show users that they fulfil the strict requirements for eGovernment solutions by displaying the eGovernment Quality Mark.

The Austrian eGovernment Quality Mark was created as a result of an initiative of the ICT Strategy Unit and the Austrian Federal Government. It is awarded exclusively by the Federal Chancellery.

---

[33] http://bbg.portal.at

All relevant information on the eGovernment Quality Mark can be found on the Federal Platform Digital Austria[34], along with a list of all current bearers.

Legal Information System

The Legal Information System of Austria is one of the most important information databases in the Web for federal and provincial law gazettes as well as decrees from the Federal Ministries. The legal publishing body of Austria for all legislation and information relevant to the law is run by the Federal Chancellery and is available for free to everyone. Particularly noteworthy is the fact that RIS has been the official source for all federal law gazettes since 2004 (not in paper form, as before). The RIS, whose beginnings reach all the way back to 1983, has been available on the Internet since 1997. It helps to streamline government and jurisdiction as well it also offers a cost-efficient and simple access to laws and legislation for both citizens and businesses.

The Legal Information System gives a comprehensive insight not only into national law, but also into European community law, and judicature of high courts, commissions and tribunals. RIS works like a search engine to provide answers to all legal questions by returning a comprehensive list of matches for search queries.

Electronic Mandates

As mentioned in the Citizens chapter, an electronic mandate can be integrated into the citizen card. The use of representatives as is common in conventional business can now be put into practice in eGovernment.

Electronic mandates are especially interesting for businesses, since mandate relationships can be stored on the citizen card, whether for authorised signatories or business managers in a company. Using the citizen card, the representatives can act on behalf of the company.

---

[34] http://www.digitales.oesterreich.gv.at/site/5422/Default.aspx

Entering agent relationships into the citizen card can be applied at the Electronic Mandate Service of the sourcePin Register Authority for the Austrian Data Protection Commission[35]. The only prerequisite is that a conventional mandate for the business or public authority already exists. This means that the existing mandate relationship will simply be represented in electronic form. It allows the representative to conduct business for the principal (the one who grants mandates) in his name.

An information service would allow principals to see who they have allowed to represent them using a citizen card. This Web service would also allow them to revoke[36] the mandate on the citizen card at any time.

Delivery

Citizens can choose to have RSa and RSb letters delivered electronically already today. However, businesses are becoming more and more receptive to this idea as well. In a few years they will be reducing the number of paper documents. However, electronic delivery should be seen as an additional service and is not intended to replace delivery of printed documents.

One of the key advantages of electronic delivery is that it is no longer necessary to go to the post office in person to pick up a delivered document. After registering with an electronic delivery service[37], business employees or their representatives can retrieve documents online, 24 hours a day, 7 days a week. Electronically delivered registered mail is held for at least 14 days. Just like conventionally delivered mail, holds can be put on delivery for short periods of time, for example, for holiday periods or sick leave. During this time, any mail that has an expiry date attached to it will not be delivered. However, with electronic delivery, it is possible to pick up mail even while on holiday because the Inbox can be checked almost anywhere, thanks to the Internet.

---

[35] https://vollmachten.stammzahlenregister.gv.at

[36] http://www.stammzahlenregister.gv.at/vollmachten.htm

[37] E.g.: https://www.zustellung.gv.at

In addition to the amount of time saved, electronic delivery also brings further cost reductions. Electronic delivery services can also send non-official documents electronically with proof of delivery.

Additional eGovernment Services

Judiciary Announcements in the Internet (EDIKT)

The Edicts Archive[38] (Ediktsdatei) on the Internet was launched in 1999 as a way to publish edicts in insolvency proceedings. It was designed to be a replacement for placing expensive announcements in newspapers and on the sometimes confusing notice boards of the courts. There is no charge for accessing the edicts archive and it is available for all citizens. Since then, the application has been expanded to include other areas of business, announcements and various lists of general interest[39].

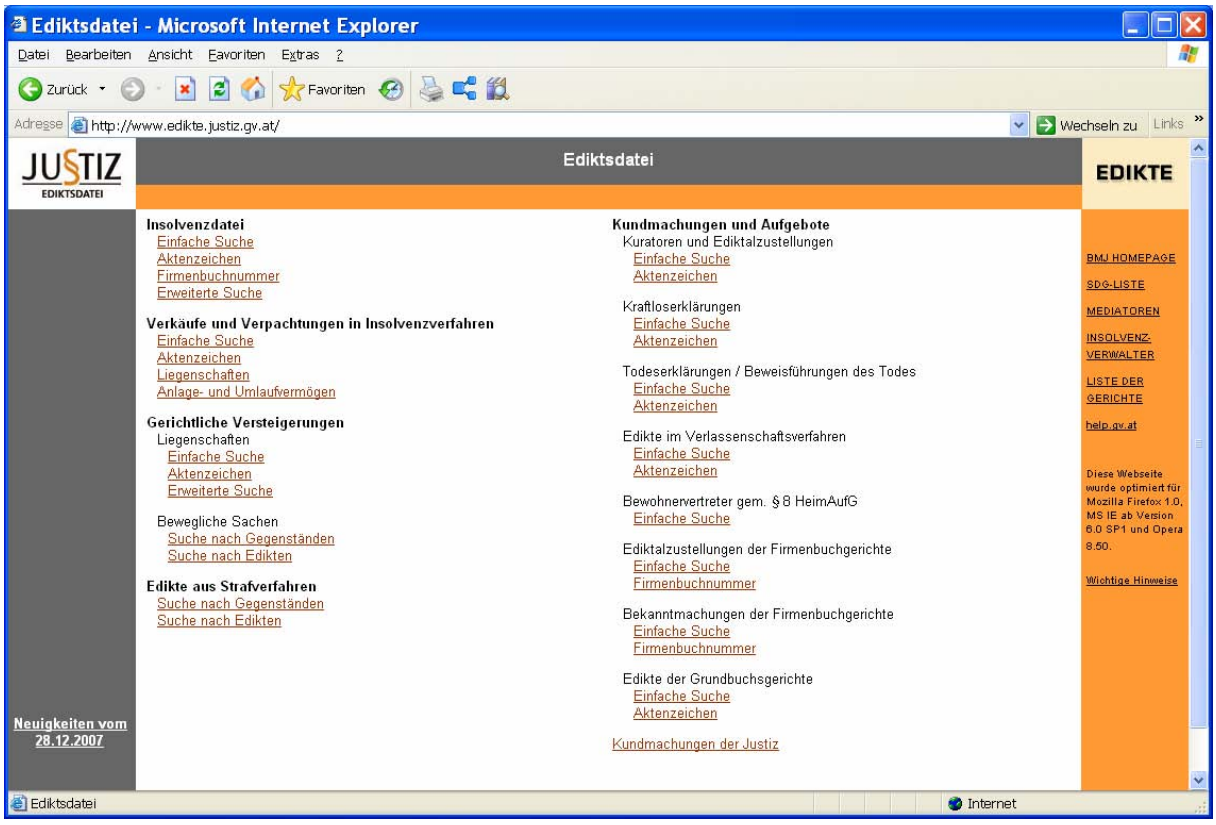


Figure 18: The Edicts Archive

---

[38] http://www.edikte.justiz.gv.at

[39] See http://www.sdgliste.justiz.gv.at, http://www.mediatorenliste.justiz.gv.at

Since the start of 2002, searches can be carried out for compulsory auctions of real estate and property, as well as announcements from the register court. In mid 2002, the Edicts Archive was expanded to include announcements from liquidators and the respective insolvency liquidator list. At the start of 2003, search functionality was added for compulsory auctions of distrained property, property owners in court proceedings, and trustees. Since 1 January 2005, almost all required announcements from court proceedings are available in the Edicts Archive.

This gives businesses quick access to all insolvency proceedings in Austria free-of-charge.

Criminal Record Certificate

A current Criminal Record Certificate is needed for many procedures. The certificate can be applied for electronically. For more information on Criminal Record Certificates , see the Citizens section in the chapter The Citizen Card in Practice.

EDM – Electronic Data Management for the Natural Resource Ministry

A special application for waste management was installed on the home page of the Ministry for Natural Resources. After the enactment of the Waste Management Law (AWG) in 2002, the waste management branch was required by law to identify and record data on assets. As a first step, an electronic register for assets and personal data (Elektronische Register für Anlagen- und Personen-Stammdaten, or eRAS) was created. This register has been in use since 10 January 2005. The "Electronic Data Management" (EDM) system, as the superstructure of eRAS, is a comprehensive system which serves as the basis for efficient eGovernment in the waste management sector.

The EDM system offers a simple system, for example, for manufacturers, and recycling and disposal centres (especially in municipalities) to enter their recycling data electronically. As well, manufacturers and disposal centres can transmit the amount of waste online. The digital transmission of CO2 emissions and inspection reports from larger industrial plants is also possible with

this system. For companies interested in this area, the respective Web pages can be found on edm.gv.at. It's worth to have a look; additional services are planned for this area in the near future, from "e-Incineration" (sector-spanning applications for transmitting emissions data together with the BMWA), to "e-Certificates" (transmission of certificates for waste evaluation).

eCustoms (Electronic Customs Clearance)

International businesses and organisations have been calling for the equalization of customs modalities in separate countries for a long time. Initiatives by the European Commission have already been started for this. Austria is one of the early adopters in electronic customs clearance, with its e-customs system.

With e-customs, businesses can take care of all formalities for customs proceedings from the comfort of their own offices. The actual location in which the wares are being stored is irrelevant. The entire process is paperless; it is no longer necessary to present a written customs application. E-customs functions 24 hours a day, 7 days a week, so businesses do not have to think about opening times at authorities offices. All essential information on e-customs is available on the homepage of the Ministry of Finance[40].

[40] https://www.bmf.gv.at/Zoll/ezoll/_start.htm

Public Authorities

One of the main goals of eGovernment is to make all public authorities available electronically from local on up to federal levels. In particular, communication should be carried out online. eGovernment will bring about a large increase in efficiency for the government, just as it does for citizens and businesses.

The city of Salzburg has developed an eGovernment solution for construction management. In the city of Gloggnitz, the civil registry office sends out notifications electronically. In Upper Austria, the entire pet registry has been published to the Web. In Burgenland, you can apply online for house building grants, and in Lower Austria you can apply online for permits for building a new house or to renovate your home.

These examples show that the possibilities for eGovernment vary widely and that practically every transaction that can be carried out in person at a public office can also be conducted online.

HELP.gv.at

The digital help site, HELP.gv.at is the first place to go for citizens and businesses to find out information on Austrian public authorities. This Internet portal is also a service point for the government itself. For mayors, secretaries of municipalities, and others in local and provincial politics, this virtual help page serves as a guide to Austrian public authorities and institutions. A multitude of transactions can be conducted directly online. Processing transactions electronically does more than just offer advantages to customers of government services; it also makes work easier for the government and brings enormous savings potential with it.

One way of supporting eGovernment is to become a partner of HELP.gv.at. This partnership is a very good opportunity for municipalities and regional and local authorities to increase their Internet presence, improve services for citizens and to offer reliable online services that have been developed by specialists. eGovernment solutions that have been developed over the past few years can be offered on the Web pages of city councils, district offices, etc. And of course, they are kept up-to-date on the latest eGovernment developments.

Currently, there are a total of 22 online services available for HELP partners with Internet forms that are sorted under the categories registry office (Standesamt), elections (Wahlen), traffic (Verkehr), taxes (Steuern), voting (Wahlen), industry (Gewerbe) and miscellaneous (Sonstiges). A list of online transactions can be found on HELP.gv.at[41]. How to conduct online transactions with public authorities is explained in the "Citizens" chapter.

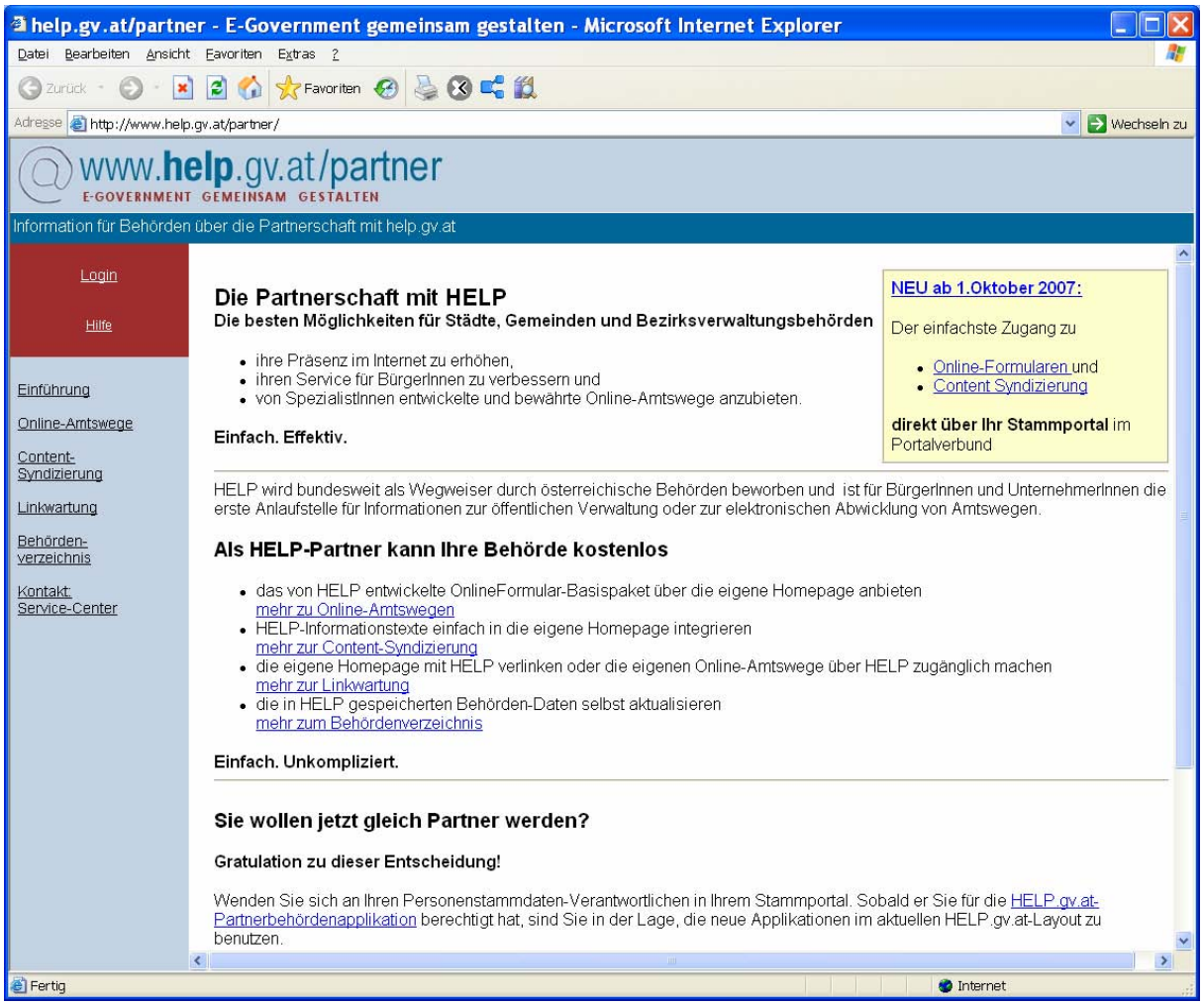


Figure 19: Information page for HELP partners

All you need to do in order to use online public authority services, which are offered as a free service from HELP.gv.at, is to register as a HELP partner and then select the desired online services. Partners only need a computer with Internet access, e-mail, an up-to-date browser and their own Web site. When ordering online services, partners must enter their Data Processing Register (DVR) number.

---

41 http://www.help.gv.at/partner

Content Syndication

The central portal of the Austrian Federal Government, HELP.gv.at, provides what is referred to as a content syndication mechanism that enables distribution and re-use of Web content. This mechanism makes it possible for content from the HELP.gv.at site to be embedded on other Web sites. The content is then updated automatically without the need for further maintenance or administration. All changes made by the central content providers are transmitted and updated automatically. The subscriber gains high-quality and up-to-date content, and at the same time it allows the provider to extend the reach of his content.

HELP.gv.at offers content sharing to partner agencies, such as municipalities, free-of-charge, whereby the partner gains additional benefits from it. Technically, it is possible to fully integrate[42] content in a content management system with only a few lines of code. This content can then be displayed using the authority's own stylesheets.

Accessibility

It is not just for the sake of fulfilling legal requirements that makes adhering to international standards, such as the Web Accessibility Initiative (WAI) Guidelines important. Rather, the goal is to build user-friendly Web service offerings that can be used with ease by everyone in the same way, simply and conveniently.

Web offerings must be able to be used without difficulty and without help from others, in order to be considered truly "barrier-free". Meeting accessibility requirements for people with special needs poses a particular challenge for information and communication technologies. Due to the diverse nature of disabilities, a multitude of aspects have to be taken into account when developing Web offerings.

---

[42] For documentation and Web presentation of an example community, see http://www.help.gv.at/applications/cs/doku

The criteria that need to be met in order to create a Web offering with the highest level of usability depends on the type of content, the purpose of the Web site and the target groups.

Various regulations build the legal framework for accessibility in Web offerings:

Article 7 of the Constitution formulates the principle of equality and also lays down a general ban on discrimination against handicapped people. The Federal Government, the provinces and municipalities must provide for the equal treatment of all people, whether handicapped or not, in all areas of daily life.

As an important result of this article of constitutional law, the Federal Act on Equal Treatment of Disabled Persons (BGStG)[43] was enacted. For Internet sites, the WAI guidelines[44] are used as criteria.

§ 1, par. 3 of the E-Government Act states that public authority Internet presences must implement accessibility features to ensure access for people with disabilities. International standards on Web accessibility should be thereby conformed with and implemented. The need for action is even more urgent for government sites in which accessibility has not been taken into account.

Further specifications are given in § 30, par. 5 of the Delivery of Official Documents Act and § 3, par. 1, line 10 of the Order of the Federal Chancellor concerning the Authorisation of Electronic Delivery Services, which reference Step A of the "Web Content

---

[43] An additional amendment was made to the Federal Act on Employment of Disabled Persons (Behinderteneinstellungsgesetz) and the Federal Disability Act (Bundesbehindertengesetz), which, along with the BGStG comprise the set of laws referred to as the "equal rights of disabled people package". In addition, individual provisions were changed in the Federal Social Security Act (Bundessozialamtsgesetz), the Act on Equal Treatment (Gleichbehandlungsgesetz), in sections of Federal Law, the Equal Treatment Commission (Gleichbehandlungskommission) and the Ombud for Equal Treatment (Gleichbehandlungsanwaltschaft), and the Federal Act on Equal Treatment in the Public Service (Bundes-Gleichbehandlungsgesetz).

[44] Web Content Accessibility Guidelines – WCAG 1.0 of WAI of the W3C

Accessibility Guidelines" for the implementation of accessibility standards for electronic delivery.

Official Signature

Public authorities have an electronic signature, just like citizens, called the Official Signature, which they can use to sign digital documents. The Official Signature is affixed to official notifications, to denote them as official documents from the public authority. The public authority can be identified by means of the Official Signature. The integrity of the document itself can be verified by the signature value.

Signature Value	50AZydZ6qx7FAFEwStqPjfGP3At5KFmaeUc+WjuCvwRVDNblqKcDfC574dykt9cO	
	Signatory	Amtsdirektor Dr. Max Mustermann
	Date/Time-UTC	2008-03-17T14:16:17Z
	Issuer-Certificate	CN=a-sign-Premium-Sig-02,OU=a-sign-Premium-Sig-02,O=A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH,C=AT
	Serial-No.	238730
	Method	urn:pdfsigfilter:bka.gv.at:text:v1.1.0
	Parameter	etsi-bka-1.0@1205763377-71964062@20020-12290-0-884-15776
Verification	Information about the verification of the electronic signature and the printout can be found at: https://demo.a-sit.at/el_signatur/verification	
Note	This document was signed with an official signature. According to § 20 E-Government-Act a printout of this document has the probative value of an official document.	

Figure 20: Potential visualisation for an Official Signature

The Official Signature must contain certain attributes, which verify the signature and confirm the validity of the document even when a copy is printed on paper. The Austrian eGovernment Act states in §19 that, in addition to the logo and the signature verification information, an indicator must be included that shows that the document comes from an authority. It would make sense for this indicator to have a standard visualisation so that everyone involved in eGovernment can easily recognize an administrative signature, whether citizen, business or public authority.

The Federal Chancellery makes modules available free-of-charge, which can be integrated into an online application or into the citizen card software on the respective government IT infrastructure.

Styleguide for Forms

However, Official Signatures are not the only elements which have to adhere to certain rules; online forms must do this as well. In the beginnings of eGovernment, forms could only be downloaded, printed, and filled-out by hand. Today, forms can be filled-out completely online, keeping in line with the requirement that no changes in media format occur in the process.

Since Web forms are the most common access point for different kinds of online eGovernment offerings, a standard presentation and visualisation is extremely important. Therefore, a Form Styleguide was developed to be used as the basis for standard design for Internet forms.

Public authorities should design their Internet forms according to the criteria in the styleguide, provided that no other design is stipulated by law. Standardised digital Government design of forms benefits eGovernment because citizens can orient themselves faster. Similarities between forms increase the recognition factor and helps users to navigate easier through online forms. Furthermore, synergetic effects can be applied to the creation of forms, as in the motto: why re-invent the wheel?

The following graphical design requirements are outlined in the styleguide:

- The online form design should contain recurring form elements such as the recipient (the public authority), the form of address (title), introductory text or explanation, hints for filling out the form, error checking, a field for comments, an acknowledgement text, as well as navigation, form recognition factors and the order of elements in the form.
- The content of the form is divided up into sections for the applicant, the address, the form fields and attachments.
- The form sections are further broken up into individual elements (section title, design, introductory texts, hints, text fields and selection fields). Guidelines on the use of fonts, lines, colours, standardised date formats, graphical elements, links and glossaries round out the styleguide.

Diacritical Symbols

In eGovernment, diacritical symbols must be taken into account. Systems must be able to recognise, process and reproduce letters that have small marks above or below, such as dots, lines, curves, or curls, which indicate a special pronunciation or emphasis.

Dual Delivery

Even in the age of eGovernment, government authorities have two basic possibilities for delivering documents: the traditional paper hardcopy delivery or the new digital one used in eGovernment. Electronic delivery of documents saves costs, speeds up delivery time and is more convenient for citizens and businesses. Since electronic delivery can only be used when the person authorized to receive the delivery consents to it, a dual delivery system was developed.

For public authorities, the advantage of the dual delivery system is that it is carried out over a single interface. The delivery can, but does not have to, be carried out electronically. With dual delivery, if the recipient is not reachable over an electronic delivery system, the delivery is carried out by a delivery service that prints the piece of correspondence on paper and sends it to the recipient by post.

Timestamping Service

In the business world, it very often comes down to adhering to deadlines and this is no exception for public authorities. Therefore it makes sense and in some cases is required by law, that in addition to the sender's signature, electronic documents must also be given a timestamp. In order to prove that a deadline has been met, it may be necessary to document electronically when a document arrived or was sent, and at which time the recipient picked it up.

The requirements for a qualifying timestamp authority are found in the Austrian Signature Act. A qualified timestamp authority is

currently being run by the Federal Office of Meteorology and Surveying[45].

eGovernment Building Blocks

As explained in chapter "Businesses", eGovernment is based on building blocks, which are easy to integrate into the online portals of local and district authorities.

When a citizen visits an authority's Web site and fills out a form, he can then sign it using his citizen card. The authority checks the signature with help from an MOA, and sends the official document either electronically or as a paper hardcopy.

The following modules are introduced as examples. For the purpose of identification, the MOA ID is used. This module enables secure login using the citizen card. Verification of the signature and document is carried out by the MOA SP. The server signature MOA SS creates the administrative signature for a public authority, and the delivery module MOA ZA ensures that documents are securely delivered electronically.

Electronic Mandates

As explained in the chapters "Citizens" and "Businesses", citizens who do not want to carry out online transactions with the citizen card themselves can authorize a representative to act on their behalf. This requires a mandate that is then saved in electronic form on the citizen card of the representative.

Citizens may also request an authorised professional representative from the authority to fill out electronic application forms for them using the citizen card. The online application form is also signed with the representative's citizen card.

[45] http://www.bev.gv.at

Electronic Record System (ELAK)

As experience has too often shown, paper files can be lost, misplaced, incorrectly filed, or land in a back corner of the archives. One of the most important developments of eGovernment for the Government is the electronic record system, called ELAK. It enables seamless communication between public authorities and other governmental service points and shortens reaction and processing time by up to 15 percent.

In 2001, the ELAK system was launched department-wide in the Austrian Ministry for Foreign Affairs and the Federal Chancellery. Since then, ELAK has been rolled out nation-wide and is also being introduced step by step in provincial governments.

The advantages of electronic record processing are obvious. ELAK substantially reduces the amount of time required for processing applications since documents no longer need to be sent back and forth between ministries and public authorities. Instead, they can be processed conveniently online. Processes are standardised and can run parallel to one another. Enquiries can be carried out directly from the desk top and the process workflow is completely transparent. With practically just a push of a button you can find out at any time of day how far the file has been processed. Furthermore, there are never any problems due to changes in the format of the file (printed copies, scans) because ELAK is based on a standardised system with uniform user interfaces.

To enable tele-working, an external access point allows users to connect to the electronic record system over the Internet. With ELAK-EXT[46] (external), remote access to the system is available using the citizen card for security.

The days of traditional paper-oriented file processing are numbered. In the meantime, paper-oriented file processing is being replaced by automated business processes.

[46] http://elak-ext.a-sit.at

eGovernment Training

Despite the prevalence of Internet, computers and mobile phones, many employees at public authorities are still shy about using what they still view as "new media". Arguments such as "it has worked up till now in paper form or by e-mail" should no longer be allowed to play a role where eGovernment is concerned. Since the importance of eGovernment is increasing on all levels of government, employees of governmental authorities should complete an eGovernment training course. This will build the basis for the successful integration of eGovernment solutions in government processes on an increasing scale.

The Austrian Federal Academy for Public Administration[47] offers practice-oriented training seminars for employees and managers at Castle Laudon. Federal, provincial and municipal employees can deepen their knowledge of electronic information, communication and transaction processes and gain practical experience in all facets of eGovernment in individual eGovernment courses.

eLaw

All the way through from the draft phase, to their introduction in parliament, and on to their enactment, the e-law concept makes provisions to ensure that legal texts follow a continuous electronic production process and that the application of technology to the text layout process is fully traceable. This makes e-law a shining example of how the electronic law creation process can substantially simplify individual steps and above all speed up the time needed starting from the drafting of a bill until it is passed. The electronic law creation process is a modern instrument that makes use of various technical components. All federal ministries are linked using Web technology to a standardised uniform workflow system that includes a standardised interface for connecting to parliament. This server-based system also includes full-text search

[47] http://www.vab.gv.at

and retrieval engine that allows users to find the legal documents they are looking for.

In this context, a reference to the Legal Information System that was introduced in the "Businesses" chapter should also be made here. In the Legal Information System (RIS), representatives for the government can call up all law texts, bill drafts, law gazettes and decrees online that appear national law or in European law communities.

Bearers of the Quality Mark

As already mentioned in the chapter "Businesses", trustworthy and secure eGovernment solutions and systems can be awarded the eGovernment Quality Mark. Those who want to earn this Mark must first fulfil certain criteria. In addition to numerous businesses which have earned the Quality Mark, the list of bearers also includes several public authorities[48].

By displaying the Quality Mark, public authorities show that their eGovernment solutions adhere to the strict requirements in the eGovernment Strategy and that their applications and products are trustworthy and secure.

Portal Group

eGovernment can only function efficiently when public authorities work closely together and cooperate on an administration-wide scale. This happens when government portals team up with each other to form a portal group and share the existing infrastructure.

The advantage of the portal group concept is that many applications are available from a single entry point. The user only needs to identify himself once when he first logs on to the portal in order to access various resources, information sources, or "digital

[48] Relevant information on the e-government quality mark as well as a list of the current bearers can be found on http://www.digitales.oesterreich.gv.at/site/5422/Default.aspx

offices". The technical term for only requiring the user to sign in once is called "single sign on".

Participation in the portal group is governed by the Portal Group Agreement (PVV)[49]. This agreement sets out the rights and duties with which the joining partners must comply. This agreement creates an environment of trust between the application providers and the base portal providers, who take care of user management.

Communication within the portal group is managed, both technically and organisationally, by the portal group protocol (PVP) and the use of security classes. Application providers determine which of their applications will be available over which portals. Keeping in accordance with all data protection regulations, they specify which administration units and employees are authorised to access which applications and define user roles with according access.

Model Application

How should an online process be built?

As mentioned already in the first chapter, long-term eGovernment solutions must be built on a modular structure, so that old modules can be replaced by new ones, as necessary. Changes to the scope or requirements, whether of a technical or legal nature, can be responded to quickly and cost effectively.

Most eGovernment processes follow the same pattern. Systematically speaking, the processes for ordering a residence registration form or a Criminal Record Certificate, or applying for a home building grant are all the same:

An electronic application form is created directly on the citizen's monitor, is automatically signed and sent to the public authority. If fees apply, they are paid electronically. If the application is approved, the document is affixed with an administrative

[49] The Portal Group Agreement and the application form for joining can be found on the Portal Group page at http://reference.E-Government.gv.at

signature and sent by the public authority to the recipient using electronic delivery. The transaction contains the same basic recurring elements throughout: an electronic form, electronic signature, electronic payment, administrative signature from the public authority and electronic delivery.

To help make the move towards eGovernment easier for public authorities and agencies, a sample process was developed. This process is used to demonstrate how individual eGovernment components can be fully integrated into existing processes. For the following example, the procedure for submitting a residence registration form online is used since it contains the most important building blocks that a part of every electronic process:

1. The application form is filled out over the Web. For this example, citizens can navigate to the virtual help site HELP.gv.at and bring up the form online.

2. Before the form is filled out, the citizen card must be inserted into the card reader.

3. Next, the applicant is authenticated after submitting his identity link.

4. The completed form is displayed along with information on any fees that must be paid.

5. A signature is added to the form when the user enters his signature pin code.

6. In the next step, a payment method is selected. If Paybox is chosen, the owner of the mobile phone receives a call from Paybox. He confirms payment by entering his Paybox pin code followed by the pound sign. The confirmation is sent to the mobile phone via SMS. If EPS 2 is selected, the user carries out the payment online using his internet banking account. Afterwards he is redirected back to the public authority application (see chapter “Electronic Payments”).

7. The applicant is shown a message that the proof of residency is ready to be picked up on the electronic delivery server.

8. In order to pick up the proof of residency, the user must authenticate himself using his citizen card.

Policies

In order for eGovernment to function properly, technical standards and, compatible software solutions are necessary. In addition, exact rules and regulations, referred to as policies, need to be set down that govern how digital communication should work.

Internet Policy

The Internet policy is the basis for Internet communication between the Federal Government, provinces and municipalities, as well as citizens and businesses. This convention describes, in a general way, possible ways to harmonise and coordinate communication from public authorities to citizens, public authorities to businesses, public authorities to other public authorities (external communication partners) and public authorities internally.

Transfer Policy

The transfer policy designates what public authorities should do when transmitting electronic data via file transfer. The following rules, amongst others, are set down in the transfer policy:

- When transmitting data by FTP, the encrypted version of this protocol (SFTP) should be used.
- For protection of privacy, the respective encrypted protocol, such as HTTPS, is to be used for the transmission of important data, in particular for personal information.
- Anonymous uploads should only be granted on public authority servers in exceptional cases, and then only temporarily. Appropriate measures must be taken to prevent any files from being downloaded from the upload directories.

E-Mail Policy

The e-mail policy contains suggestions on what public authority employees should take into consideration when sending electronic data by e-mail. The goal of this policy is to define a

minimum standard for public authorities when using e-mail as a medium. The e-mail policy points out the following measures:

- Contact with citizens should, whenever possible, be carried over a Web interface, for example, using a Web form.
- E-mails that are sent from the Government should be clearly marked with a signature, whenever technically possible.
- E-mails should always be sent in plain text rather than HTML format.

Domain Policy

The domain policy aims to present a uniform picture on public authority Web sites, and to guarantee that security and organisational requirements are complied with.

Every Web site presence must include legal contact information, a contact address and search functionality. Optimally, it would also make use of electronic forms and have a sitemap. Particular emphasis should also be placed on adherence to WAI standards for accessibility with regards to page layout.

gv.at Domain Registration Policy

All individual public authority Web sites should appear under a single domain, namely "gv.at". This measure should build up trust amongst users, so that they can be confident that the service or information on the site is official. The "public authority" should already be recognizable by the name in the address field of the browser. The domain names for gv.at are given out by the Federal Chancellery free-of-charge to public authorities. Technical administration is carried out by Vienna City Magistrate. In addition to increasing citizens' trust, gv.at domains offer protection from domain name grabbing[50]. Furthermore, gv.at Web sites can be accessed anytime day or night for free from the approximately

[50] In domain grabbing, third-parties reserve domain names in hopes of making a profit by selling them later

850 multimedia terminals or over any of the numerous WLAN access points.

Directory Service

Today, citizens, businesses and public authority employees have to read in agency calendars, provincial notices and various other publications to keep up-to-date on the areas of responsibility in public administration. In the future, a directory service will deliver an overview of all public authorities and their areas of responsibility. This service will contain all relevant contact information and descriptions which can be queried in standard search. It is also possible to access this information from the public authority directory on HELP.gv.at.

Keeping the directory current and as complete as possible requires the cooperation of all public authorities, which have to deliver up-to-date data on a regular basis. The directory takes on special importance with regards to the service guidelines of the EU by allowing the responsible federal, city or municipal authority to be searched for and found.

Register

Address Register

The address register is maintained by the Federal Office of Meteorology and Surveying and contains all addresses of public authorities in Austria along with their spatial coordinates. Individual addresses in the address registry can be looked up free-of-charge. Additional products can be purchased which contain different sets of high quality geo-data from Austria, such as a cadastral map or Austrian road maps.

Maintenance of the data in the address registry is carried out using the online application ADR-GWR, which is also used to maintain the buildings and appartments register.

Register of Buildings and Appartments (GWR)

The GWR is a database run by Statistics Austria, which is used for gathering public statistics. Municipal authorities enter data on construction sites and future projects, although data on appartments is not used for calculating statistics. For example, the Central Register of Residence accesses the Buildings and Appartments Register to register new addresses and to make changes to existing address. This helps to preserve the quality of the registered addresses.

Through frequent use and the experiences gained from the municipal authorities when using the address GWR online application, the need for improvements was recognized in the areas of usability, the data model and the user interface. Currently, an extensive redesign of the application is underway along with the project GWRII, which strives to create a better user interface, amongst other things. Along with this, standardisation of building codes in provincial laws will be achieved. The goal for the future is that the GWR will become a dependable source of data for various public administration applications. On the basis of the buildings data from the GWR, energy certificates are created, standard values are measured, and recommended amounts for period payments are calculated.

Legal Basis

The legal scope of eGovernment is not confined to a single law or regulation, but rather is defined in broader terms. Regulations that deal with eGovernment are found in numerous federal and provincial law books.

However, the basic framework for eGovernment is comprised of a relatively manageable set of laws. They are the EGovernment Act (E-GovG), General Administrative Procedures Act (AVG), Service of Official Documents Act (ZustG) and the Electronic Signature Act (SigG). These laws are further supplemented by other acts and regulations. In addition to ensuring data protection and guaranteeing a high standard of security, eGovernment should serve to simplify citizens' lives.

In a Europe-wide comparison, Austria was one of the first Member States of the European Union to pass comprehensive legal regulations in the area of eGovernment. The eGovernment Act is viewed as an example throughout Europe. For this reason a working version of this document is available in English to give all those interested an insight into the individual regulations on an international level.

eGovernment Act (E-GovG)

The eGovernment Act is the core of Austrian laws on eGovernment. It was enacted on 1 March 2004 and on 1 January 2008, the first amendment was passed. This law serves as the legal basis for eGovernment services. It enables closer cooperation between all authorities that provide eGovernment services and gives them the opportunity for networking together. Many mechanisms such as the citizen card, sector-specific personal identifiers and electronic delivery of documents are also able to be put to use in the private sector.

The most important principles of eGovernment law are:

- Freedom of choice for users in selecting the means of communication when contacting with public authorities;
- Security and improved legal protection provided by appropriate technical measures such as the citizen card

- Unhindered access for people with special needs to public administration information and services. International standards must be adhered to and access to Internet sites must be provided.

The following sections contain a brief overview of the essential regulations.

Citizen Card

The citizen card is electronic identification for the Internet. People can use it for identifying themselves by digital means to a public authority. It allows them to be uniquely identified and authenticated where required by law. The citizen card contains a qualified electronic signature that makes it possible to sign forms or contracts which normally require a personal handwritten signature. While practical for doing business with public authorities, the citizen card can also be put to use in personal matters, for example, in order to increase the security of Internet transactions or for e-banking.

The citizen card is available in many different formats, since it does not depend on a particular type of technology and does not require one specific type of card. In most cases, the carrier medium is a chipcard (such as the e-card). It is essential that the citizen card contains a qualified electronic signature and an identity link that contains the associated security data and functions, as well as any data on mandates which may have been granted.

sourcePIN

Due to the strict regulations on data protection in Austria, in place of using the ZMR number (number from the Central Register of Residents), a highly encrypted and non-reversible derivation of the ZMR number is used to calculate the sourcePIN. For people who are not registered in the central register, the sourcePIN is created using their registration number from the supplementary register. The sourcePIN for natural persons may only be stored on their citizen card. For legal persons, the entry number in the Register of Company Names (Firmenbuch) or the Central Register of

Associations (Zentrales Vereinsregister) or the registration number in the Supplementary Register is used as the sourcePIN.

Identity Link

The identity link is used to create a unique link between the citizen card and its rightful owner. More specifically, the sourcePIN Register Authority verifies by way of an electronic signature that a link has been established between the citizen card holder and his or her sourcePIN for the purposes of unique identification. The identity link is entered on the citizen card.

Electronic Mandates

Individuals may authorise another person to submit applications on their behalf. In such cases, the sourcePIN Register Authority stores the mandate, including any limitations it may contain, and the sourcePIN of the person being represented on the representative's citizen card. Mandates can also be used by professional representatives.

Sector-Specific Personal Identifiers

In order to ensure the protection of data, authorities are not allowed to store the sourcePINs of natural persons in their applications. The authorities may identify natural persons only by their sector-specific personal identifier (ssPIN). The ssPINs are derived from the respective person's sourcePIN. This process must be irreversible and it must not be possible to calculate the original sourcePIN back from the ssPIN. An ssPIN is valid only for the sector of activity of the authority under which the initiated procedure falls. Personal identifiers from other sectors may only be used in encrypted form. In order to generate an ssPIN, the sourcePIN is needed. The sourcePIN may only be used to generate the ssPIN - using the citizen card - with the agreement of the person concerned. If the sourcePIN is unknown, only the sourcePIN Register Authority may generate an ssPIN without a citizen card, and it may do so only in certain circumstances.

sourcePIN Register

The sourcePINs required for the unique identification of persons are available from the sourcePIN Register. Technically, the sourcePIN register is a virtual register, meaning that sourcePINs are only generated when required and are deleted afterwards. The functions of the sourcePIN Register Authority are carried out by the Data Protection Commission.

Supplementary Register

All natural persons who do not have a registered address in Austria and legal persons who do not appear in the Register of Company Names or in the Central Register of Associations can register themselves in the supplementary registers in order to participate in eGovernment.

Standard Document Register

Until now, citizens and businesses were required to prove certain information by providing documents, such as birth certificates, proof of citizenship, or documents from the Register of Company Names in order to conduct certain transactions. With electronic administration, this is no longer necessary in many cases, since electronic data that is already stored in the registers is allowed to be used. When a person registers with an authority, the authority verifies the accuracy of the personal and nationality data by inspecting the relevant documents (standard documents). It then informs the Central Register of Residents that the information is accurate. A person may request that the accuracy of the information be recorded, even in cases where no registration procedure is being conducted, provided that he or she can provide proof of the accuracy of the information by presenting the relevant documents. Thus, certain information need no longer be presented by the person concerned but can, with the person's consent, be directly requested by the authority from the Central Register of Residents.

Official Signature

Persons conducting transactions with public administration must be able to rely on the authenticity of documents they receive from the authorities. The Official Signature is an advanced electronic signature affixed by an authority to an administrative notice or document. This makes it easy to recognise electronic documents issued by authorities. Not only can the authenticity of the document be verified by means of the Official Signature, the printed version of it is also treated as being equivalent to the official document by the authorities.

SourcePIN Register Regulation

The sourcePIN Register Regulation specifies the responsibilities of the sourcePIN Register Authority which are necessary for the implementation of the citizen card concept and the cooperation with its service providers. The main provisions deal with the following:

- The process to create identity links, including setting down the duties of citizen card registration agents, the validation of identity, and the identity link dataset. The regulation also lays down that a compliant citizen card environment needs to support an interface that can bind the citizen card to the application. This interface is defined and published by the sourcePIN Register Authority.

- The transformation of sector-specific personal identifiers (ssPIN) into ssPINs of other authorities, the creation of ssPINs for specific authorities and for data applications in the public sector. The ssPIN Register Authority has an interface to create and transform ssPINs which it makes available to public authorities. This interface is also accessible via the portal network of public authorities. Each request to calculate an ssPIN is recorded by the sourcePIN Register Authority.

- The electronic representation of mandates on citizen card. One of the remarkable achievements of the citizen card concept is the possibility to represent mandates electronically. The sourcePIN Register Authority electronically signs a mandate

representation dataset and thus prevents forgery of such datasets stored in a citizen card. A service to revoke mandates online over the Internet will be provided by the sourcePIN authority.[51]

eGovernment Sectors Delimitation Regulation

For the purpose of generating sector-specific personal identifiers, each public sector data application needs to be assigned to a sector of State activity. The eGovernment Sector Delimitation Regulation defines the designations and the sector-identifiers.

Supplementary Register Regulation

This regulation plays an important role in the implementation of the citizen card concept in that it enables natural persons and other affected parties to be registered in the supplementary register, who, due to legal restrictions, are not allowed to be entered into the primary registers (ZMR, Register of Company Names, Central Register of Associations).

The supplementary register is separated into two: one register for natural persons and another one for "other concerned parties".

The eGovernment Act allows the sourcePIN Register Authority to take over the duties of service provider for the Federal Ministry of Interior for the supplementary register for natural persons and for the Federal Ministry of Finance for the second supplementary register.

The Electronic Signature Law (SigG)

The electronic signature law lays down the fundamental principles of electronic signatures in accordance with the European signature guidelines. The electronic signature law differentiates between three types of signatures: simple, advanced and qualified. The citizen card uses a qualified signature. According to

[51] http://www.stammzahlenregister.gv.at/vollmachten.htm

the signature law, a qualified signature is equal to that of a handwritten signature. This means that you can sign electronic contracts with a qualified signature and they will be as legally binding as if the contract was signed by hand. The electronic signature law also specifies requirements for businesses that issue qualified certificates (certificate providers), as well as regulations for the authentication of foreign certificates.

General Administrative Procedures Act (AVG)

As the name implies, the General Administrative Procedures Act (Allgemeine Verwaltungsverfahrensgesetz) lays down the basic principles of administrative procedures. Article 13 of the AVG is relevant to eGovernment in that it regulates the ways with which public authorities and citizens can communicate with each other, such the transmission of applications by e-mail or Web forms. The authority's Web site must list the addresses that application forms can be sent to, whether an electronic signature is needed, and which formats are recommended or required for the application (§13, par.2). Opening times must also be published on the site (§13, par. 5 AVG).

Starting 1 January 2011, written copies of public authority transactions or of electronic created documents require a handwritten signature, certification or official signature. From this point on, all electronic documents from the public authority are required to have an official signature affixed to them.

Service of Documents Act (ZustG)

The Service of Documents Act governs the delivery of all documents, such as official notices, which government authorities are required by law to send out. In the electronic world and paper world alike (§3, ZustG), a differentiation is made between deliveries that require proof of delivery, by which the recipient or his representative confirms the delivery with a signature, and deliveries where no proof is required.

Proof of delivery (§35 ZustG) is carried out via an electronic delivery service. This service is available from delivery service providers that have been approved by the Federal Chancellor. It

allows customers (citizens and businesses) to register with their citizen card to confirm that they want to receive administrative documents electronically. A list of these delivery service providers is published by the Federal Chancellor on the Web. Registering with a delivery service is sufficient notice in order to receive admininstrative documents. However, neither citizens nor public authorities are obliged to use an electronic delivery service if they do not wish. When an authority needs to send a document using a delivery service, the recipient is notified up to two times by electronic means (e.g., by e-mail or SMS) that a document is ready to be collected. A third notification can also be sent out by post. The delivery is confirmed as soon as the document is picked up by the recipient. Proof of delivery is verified when the document is retrieved using the recipient's citizen card, or when an explicit agreement exists that allows documents to picked up automatically using an automated signature. Confirmation of delivery is also made even if the document is not picked up by the recipient.

For cases when an application form is sent and received in the same session of the Web application while the recipient is using the citizen card, proof of delivery for the document that was received is confirmed by "immediate electronic delivery" according to §37a of the ZustG.

Electronic deliveries without proof of delivery can be confirmed nonetheless using the above mentioned methods ("electronic delivery service" with "immediate electronic delivery", although it is not necessary for the citizen card to be used), or by using the "electronic communication system from the authority" or an "electronic delivery address".

Starting 1 January 2009, in accordance with §37 of the ZustG, before documents can be delivered using an individual "electronic communication service from the authority" (e.g., the Databox in FinanzOnline), a delivery using an electronic delivery service must be attempted first. Only afterwards is it allowed for deliveries to be sent out to recipients that are registered on the authority's system. This includes cases in which an electronic delivery service cannot be used because the recipient is not registered with one.

Electronic delivery can also be carried in cases where the recipient gives an e-mail address to the public authority as his "electronic delivery address" during a procedure (§ 37 ZustG). However, the use of electronic delivery may only be used during this procedure and not for any other procedures which are carried out later.

Delivery Service Regulation

The Delivery Service Regulation further defines the admission standards that are given in §30 of the Service of Documents Act. These standards include criteria for assessing the technical and organisational ability of delivery services and the reliability of data protection aspects in particular. The technical requirements that are to be fulfilled by delivery services are contained in an annex to the Delivery Service Regulation, and are to be published in the Internet.

Delivery Forms Regulation

The Delivery Forms Regulation defines the forms for the first and second notifications, which are sent electronically, as well as for the third and final notification, which is sent by postal delivery to the recipient's delivery address (e.g., home address), if one has been provided.

Infrastructure

Fundamentals

A modern, secure, flexible and expandable IT infrastructure is essential for eGovernment. In the process of digitising public administration and services, recommendations were developed, and standards were adapted and implemented. These measures are introduced in the following sections.

IT Security and Data Protection

The federal security strategy and its goals are published in the Austrian Handbook for Information Security[52] (Informationssicherheitshandbuch). One aspect of this strategy is concerned with identifying and authenticating users in a secure way that complies with data protection regulations. These functions are illustrated by the *citizen card concept*. The citizen card software is freely available for use in eGovernment. The central components of the citizen card concept are the qualified electronic signature and the system of unique and data protection conform personal identifiers which are derived from the sourcePIN.

Depending on the requirements of the application or authority, electronic communications between citizens and the authorities can take place with or without the citizens having to uniquely identify themselves. These security requirements can be classified into two levels, which describe the necessary elements for the ICT security infrastructure for electronic administrative processes.

- Level I: On this level, there is no particular need for security. A one-way authenticated TLS (Transport Layer Security) connection ensures basic security with use of the authority's identification attribute in the certificate. Authentication occurs on the server-side only, which ensures customers of the genuine nature of the services being offered by the public authority, whereas the customers are not required to identify themselves.

[52] http://www.a-sit.at/de/sicherheitsbegleitung/sicherheitshandbuch/index.php

- Level II: On this level, communication in administrative processes must be authenticated. Communication between clients and the server is encrypted, thereby ensuring authenticity and confidentiality of the content. In practice, this level of security is carried out by identification and authentification of the citizen using the citizen card and the MOA ID.

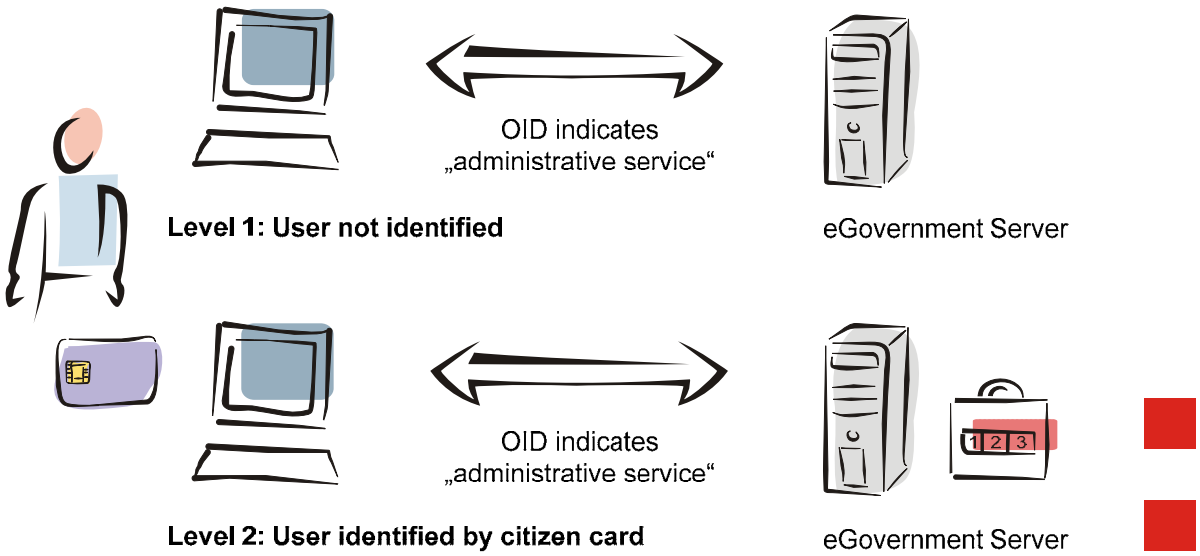


Figure 21: Security and identification in eGovernment

Public Key Infrastructure

The public key infrastructure (PKI) forms the basis for authentification and identification of electronic communication with public authorities. This technology is based on the principles of asymmetric encryption. Data is processed with the help of two keys, a private and a public one, which together form a complentary pair. Encryption and decryption of the data is carried out using these complementary keys. A PKI is responsible for the creation, distribution and revocation of key pairs.

As part of the scope of PKI, keys and information about the key's owner can be encapsulated in a *certificate* and signed by the certificate authority. This allows the ownership of keys, the terms and conditions under which they are created, and the security requirements to be kept under control, thereby increasing the trustworthiness of the system.

The most important use of a PKI is the electronic signature, in which, in case of RSA, a representation (hash value[53]) of a message is encrypted using the sender's private key. The sender's public key is available together with his certificate and can be used for verification purposes. This allows the message to be reliably linked (authentification) to the person who signed it (signatory). It is important for signatories to treat the keys for their digital signatures responsibly. Information needed for creating signatures (e.g., signature PIN) should not be accessible to others.

With the use of the electronic signature on the basis of a PKI, a legally binding system of communication between public authorities and citizens or between authorities themselves can be implemented.

Certificates and signatures can be used for many purposes in public administration:

- Qualified certificates for cases requiring a qualified electronic signature
- Qualified and advanced signatures for cases requiring an administrative signature
- Certificates for Web services for the partly automated signature of data
- Server certificates used to digitally authenticate a server
- E-mail certificates to increase the trustworthiness of e-mails sent by public authorities
- Encryption certificates for the encryption of data
- Certificates for special applications (digital tachograph, electronic passport, etc.)

[53] http://en.wikipedia.org/wiki/Hash_function

Citizen Card Concept

As already mentioned, the citizen card is an essential component of ICT security in eGovernment. The citizen card concept offers functionality for the identification and authentification. It is comprised of the following elements:

Citizen Card

The citizen card token is the element that ensures that the user has solitary control when accessing applications. The token can take the form of, for example, a chip on a plastic card, such as the e-card. The token controls the calculation of cryptographic functions and access to the data on the citizen card. The data stored on the citizen card includes the user's first and last names, date of birth and the keys required for creating signatures. In a separately controlled area, the sourcePIN for deriving sector-specific personal identifiers, and, where applicable, data on authority to act as a representative is stored as signed data according to applicable standards:

- Cryptographic operations: Various mathematical operations and algorithms are used for creating signatures. The Signature Act of 2008 specifies operations and their parameters, in accordance with current security standards.
- Key pairs for signatures and encryption: In addition to the key pair that is used for creating qualified electronic signatures as per signature law, a second key pair is usually stored on the citizen card (in chip card form) which can be used for other purposes. Although this key pair is not essential for eGovernment transactions in itself, it can be used for data encryption or for logging on to Windows.
- Identity link: The person's first and last names, date of birth and the sourcePIN are signed by the SourcePIN Register Authority and saved on the citizen card. The fact that the data is signed confirms the identity of the user.
- Optional mandate data sets: These data sets bind the sourcePIN of the representative to the sourcePIN of the person

who granted the mandate. It contains an index to revoke the mandate representation agreement, if the need should arise.

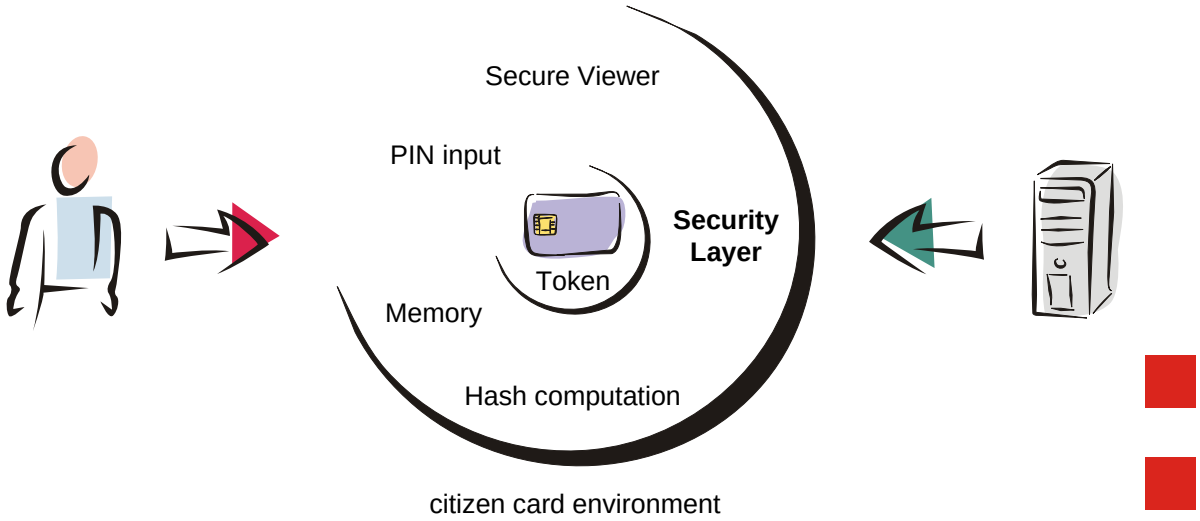


Figure 22: Citizen card environment and token

Since the citizen card environment is built upon open standards, it allows all signature cards that fulfil citizen card specifications and legal requirements to be used as a citizen card.

The same thing applies for foreign "citizen cards". This refers to any foreign electronic identification cards that are built on the basis of electronic signatures, for example, the Belgian electronic identity card.

In order for these kinds of electronic identities to be accepted as valid citizen cards in Austrian eGovernment, the owner must apply for an identity link and then store it on the card. The identity link is built on the basis of the person's entry in the supplementary register. If the person does not already have an entry, he must apply for one first. In addition, the signature card must be recognized as being equivalent to the citizen card as set down in §6, par. 5 of the E-GovG.

Security Layer

For the implementation of the citizen card concept, a so-called *security layer* was specified. The security layer is the interface between an application, such as a Web application, and the signature card. It offers access to the token's functions for the purposes of identification, signatures and encryption. The security

layer is embedded in the citizen card environment software as *middleware*[54] and fulfils the following requirements:

- Hardware and technology-independent: The application only has access to the logical view of the functionality and does not see how the token is implemented. Therefore, the type of token which carries out the signature function, whether on a smartcard, USB stick or Web service, should be irrelevant to the application.
- Independent of cryptographic algorithms: Over time, scientific and technological advances lessen the security of cryptographic operations. Therefore, these algorithms must be able to be replaced without impacting the application.

Display of Documents and the Formats Used

An essential component of any signature solution is the ability to display the message to be signed in a way that can be trusted by the user. It must ensure that the message to be signed does not contain any hidden content or any dynamic elements which could later change the content.

This guarantees that the content to be signed (texts, forms, documents, etc.) can always be processed and displayed in the same way by the recipient who is verifying the signature.

For this reason, a uniform standard for the display format[55] was developed to ensure that different implementations of the citizen card software are able to do this. The specifications for the display format are based on international standards for displaying data, XHTML 1.1[56] and CSS 2[57].

---

[54] http://en.wikipedia.org/wiki/Middleware

[55] http://www.buergerkarte.at/konzept/securitylayer/spezifikation/aktuell/viewerformat/ViewerFormat.html

[56] http://www.w3.org/TR/2001/REC-xhtml11-20010531/

[57] http://www.w3.org/TR/1998/REC-CSS2-19980512/

Personal Identifiers

sourcePINs for natural persons

In order to identify a person involved in an electronic process, there needs to be an attribute that uniquely identifies them. Since a name alone is not enough to uniquely identify someone, each person is assigned an additional identifier. In Austria, every citizen that has a residence registered in the country has a ZMR number stored in the Central Register of Residents. However, since the ZMR number is subject to special legal regulations, it cannot be used for identification purposes in eGovernment. Instead, a strong encryption process is used to derive a sourcePIN from the ZMR number. Unlike the ZMR number, the sourcePIN is allowed to be stored on the citizen card which guarantees its protection.

0	Base number	000247681888 (Ex: ZMR number, 12-digit decimal number)
1	Binary representation	00 0E C3 53 60 (5 byte, hexadecimal number)
2	Expanded to 128 Bit	00 0E C3 53 60 FF 00 0E C3 53 60 00 0E C3 53 60 (16 byte, seed value, set to 'FF' as an example)
3	Triple-DES encryption, hexadecimal	42 AD 37 74 FA E0 70 7B 31 DC 6D 25 29 21 FA 49 (16 byte)
4	sourcePIN, Base64	Qq03dPrgcHsx3G0lKSH6SQ== (24 characters)

Table 1: Deriving a sourcePIN. (Source: Hollosi/Hörbe, sourcePIN-ssPIN Algorithm V1.1.1)

Due to the mathematical algorithm used, the process is irreversible. The individual steps are: The 12-digit ZMR number is transformed into its binary equivalent (1). To increase the strength of the encryption, the calculation base is increased and a secret seed value is added to it (2). The expanded binary number is encrypted with a secret key using a triple DES algorithm[58] (3). The

[58] http://en.wikipedia.org/wiki/Data_Encryption_Standard

Base64 standard[59] is used to encode the result to make the sourcePIN easier to read by character-oriented systems (4).

The final result is an alphanumeric series of 24 characters. The only place where this number is allowed to be permanently stored is on the citizen card. The sourcePIN Register Authority is responsible for the application that derives the sourcePINs. The secret key used for deriving sourcePINs is only known to the sourcePIN Register Authority.

sourcePINs for non-natural persons

For non-natural and legal persons, the entry number in the Supplementary Register, Register of Company Names or the Central Register of Associations is used as the basis for deriving the sourcePIN. Since these identifiers are public, they can be written without its derivation in plain text communications.

Sector-specific personal identifiers

Since sourcePINs can only be stored on a citizen card, additional identifiers are needed that are allowed to be stored in databases during public authority processes.

One fact that must be considered is that public administration is divided into legally defined sectors of State activity[60]. The eGovernment Act states that different identifiers must be used for each sector.

For this reason, a sector-specific personal identifier (ssPIN) is derived from the sourcePIN. The derivation is based on an irreversible cryptographic operation to ensure that the sourcePIN cannot be calculated back from the derived identifier.

---

[59] http://en.wikipedia.org/wiki/Base64

[60] See eGovernment Sectors Delimitation Regulation

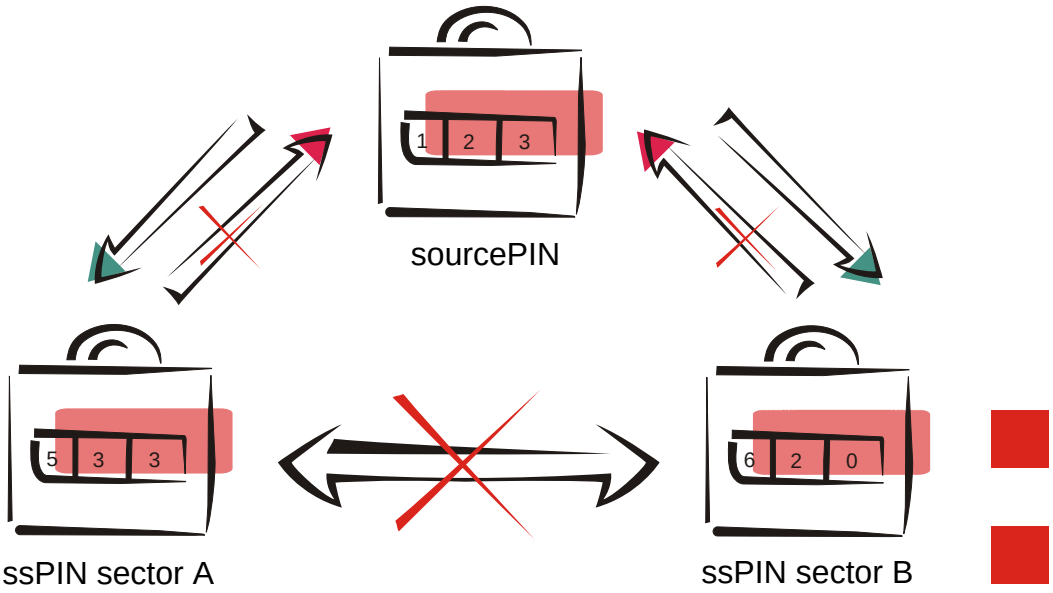


Figure 23: Identifiers derived for separate sectors

In the first step of deriving an ssPIN, a series of characters is built from the sourcePIN and the abbreviation for the procedural sector (1). This series of characters is used to compute a secure irreversible cryptographic number using a specific hash algorithm[61] (2). For readability purposes, the ssPIN is encoded in the base64 standard (3). Unlike the sourcePIN, this number is allowed to be stored in administrative processes.

The authorities can use the same ssPIN to retrieve the citizen's data stored within the same sector, for example, if they need to the citizen's records or use it to pre-fill forms. However, authorities do not have access to ssPINs from other sectors, nor do they know the sourcePIN from which ssPINs can be calculated for other sectors.

This provides the most protection for individual's personal information, which is an important requirement for eliciting citizens' trust in the many possibilities for electronic services.

[61] http://en.wikipedia.org/wiki/Cryptographic_hash_function

0	sourcePIN, Base64	Qq03dPrgcHsx3G0lKSH6SQ== (24 characters)
1	Sector abbreviation	BW (ISO-8859-1, Example: Bauen und Wohnen
2	Data for the hash calculation	Qq03dPrgcHsx3G0lKSH6SQ==+urn:publicid:gv.at:cdid+BW
3	Hash value with SHA-1, hexadecimal	8FF3717514 21A7EB4DC8 4F56847741 498BB2DE10 (5 x 32bit; as hexadecimal number)
4	ssPIN, Base64	j/NxdRQhp+tNyE9WhHdBSYuy3hA= (28 characters)

Table 2: Deriving an ssPIN. **(Source: Hollosi/Hörbe, sourcePIN-ssPIN-Algorithm V1.1.1)**

Encrypted sector-specific personal identifiers

Administrative processes often require that authorities from different sectors of the administration work together, for example, the building sector and environment sector during construction of a facility or building. To facilitate this type of cooperation, there needs to be a way to consolidate data that is saved in different sectors under different ssPINs. If an authority requires an ssPIN from another sector for identification purposes, they can request it from the sourcePIN Register Authority. They send the ssPIN to the authority that requested it in encrypted form. The ssPIN can only be decrypted by the public authority that is responsible for the foreign authority. The ssPIN must be based on an asymmetric encryption (RSA/1024 Bit) process and computed in a way that makes it impossible to trace it back to the person.

Personal identifier for the private sector

The method of deriving ssPINs from the sourcePIN for the purpose of identifying persons can also be used by the private sector for e-business. The derivation process for sector-specific identifiers for the private sector (private ssPIN) is carried out in the same way as for the ssPIN. For the calculation of the private ssPIN, the sourcePIN of the legal person who wants to identify customers is used in place of the abbreviation of the procedural sector. This process creates a unique identifier that is comprised of the sourcePINs of both communications partners. Since the ssPIN can only be derived from the sourcePIN, which is protected, it ensures that the ssPIN can only be created for use in the private sector with permission of the person concerned. The ssPIN can only be

derived by the citizen card environment on the user's system using his sourcePIN. Each business and organisation is assigned to its own sector based on its registration number in the Register of Company Names or Register of Associations, respectively.

Electronic mandates

With an electronic mandate agreement, individuals can use their citizen card to carry out procedures on someone else's behalf. The representative can be either a natural or legal person. This can be the case for natural persons who do not wish or are not able to conduct online procedures with the citizen card themselves, and therefore entrust someone to conduct procedures on their behalf.

For legal persons, it is possible to authorize a representative to carry out administrative processes on their behalf. The electronic mandate makes it possible to uniquely identify the legal person who is being represented.

The specified XML data structure of the electronic mandate[62] contains the identification data for the principal (the person to be represented) and the representative. There are various options for the mandate agreement: on the one hand it can be registered without any restrictions, for example with full mandate authority rights, or it can contain restrictions for the period of validity or transaction limits. Within the scope of eGovernment cooperation, standard text blocks will be defined that can be combined to create a complex mandate agreement which still can be checked automatically.

In order to represent somebody electronically, a proxy agreement must be stored on the citizen card. A Web form from the sourcePIN Register Authority allows the principal to prepare the proxy agreement and specify a representative. The principal selects the type, specifies any limitations and then signs it. The proxy agreement is sent electronically to the representative, who accepts the prepared agreement and applies to have it entered on his citizen card.

---

[62] http://www.ref.gv.at/Buergerkarte___Elektronische_V.961.0.html

If the principal is a legal person, the representative is activated and can apply to have the proxy agreement entered on his card. The sourcePIN Register Authority checks the proxy relationship in the according register (e.g., Register of Company Names) and confirms the proxy agreement. The requested proxy is made available to the representative for download onto his citizen card. The representative can call up the proxy agreement using the proxy application from the sourcePIN Register.

Professional Representation

For professional representatives and administrative officials, who have authority to act in accordance with legal regulations[63], have a specific attribute on their professional certificate that identifies them as an authorised representative. From a technical point of view, this attribute is implemented as a certificate extension according to the X.509 standard and is registered as a unique object under its object identifier (OID). The OID is an essential component for carrying out authentification and identification in eGovernment because it can be used to reliably represent a defined attribute of the signatory, such as his occupational category. Object identifiers are stored directly in the signature certificate. They can be automatically processed using a signature, for example by MOA ID, during authentification to inform the application that the user can conduct transactions for himself as well as on behalf of a third-party. Since the issuance and revocation of the certificate of the individual representative is carried out by his professional representation (e.g. the Austrian Chamber of Civil Law Notaries), a valid certificate accurately represents the occupational category and proxy authority relationship.

On the technical side, the same proxy authority data structure is used during the logging in process for professional representation and when citizen cards from other Member States are used. A service from the sourcePIN Register enters the data of the principal into the proxy structure and then returns it to the authentification component of the application. In this way, the infrastructure

[63] §5 (3) E-Government Act

required for the electronic process (MOA ID) can be kept as simple as possible.

Accessibility

Along with the advantages and opportunities that the information age brings the danger arises that socially disadvantaged people and those with special needs will be excluded from using new media channels and technologies. This phenomenon is known as the *digital divide*[64]. To prevent this from occurring, all Web content should made available for everyone through adherence to the guidelines of the *Web Accessibility Initiative (WAI).* Administrative processes should become easier to use in particular for the elderly or people with disabilities by taking their special needs into consideration.

Accessibility on the EU level

Austria has announced its plans to implement WAI guidelines to the EU, and thus they are an inherent part of the eGovernment strategy. This means that the minimum standards as stated in the Web Content Accessibility Guidelines 1.0 must be fulfilled on a national level.

Specifically, Member States must:

- speed up the process of adapting Web content to the WAI guidelines
- achieve WAI conformity on all levels – federal, regional and local.
- take WAI conformity into consideration when commissioning the creation of Web content by external parties
- strengthen dialogue with appropriate interest groups, such as disabled and senior organisations
- improve the access to technology for people with disabilities
- remove technical, legal and other barriers to enable real involvement in a knowledge-based economy and society

[64] http://en.wikipedia.org/wiki/Digital_divide

Legal Framework in Austria

EU level requirements for accessibility and barrier-free access for Web sites and services is a driving factor behind accessibility. This issue is addressed in the following laws, regulations and legal frameworks in Austria:

Federal Constitution

Article 7 of the Federal Constitution states the principle of equal treatment and contains a specific ban on discrimination against disabled persons. It also expresses a common goal that it is the duty of law makers to ensure virtual equality for all. The Federal Government, the provinces, and municipalities avow to uphold the equal treatment of disabled and non-disabled persons in all areas of daily life.

Laws for the Equal Treatment of Disabled Persons

The Federal Act on Equal Treatment of Disabled Persons (BGStG) is an important step towards realising the requirements set down in the constitution. It contains, amongst other provisions, a prohibition against discrimination and sets the criteria for what constitutes discrimination and states the legal consequences that stem from it.

§6, par. 5 of the Equal Treatment of Disabled Persons Act states that technical equipment, information processing systems, and other aspects of life can only be considered barrier-free when they can be used normally by disabled persons without difficulty and without the need for help from others. The standard of measure for Web offerings is taken from the WAI guidelines.

This definition of barrier-free access went into effect on 1 January 2006 and is to be applied to legal relationships including their initiation and rationale as per §2, par. 2 of the BGStG. This means that in general, even non-official Web offerings must conform to these requirements. However, the decision whether a non-official site should be checked for conformity is handled on a case by case basis according to §6.

§9 of the BGStG provides for compensatory damages as legal consequences in discrimination cases. Claims must go through an arbitration process prior to being brought before the courts (§10, par.2 BGStG).

eGovernment Act

In §1, par.3 of the eGovernment Act (E-GovG), the goal for implementing barrier-free access in official Internet sites for persons with disabilities is set down by law. They are required to implement and conform to international standards on Web accessibility. The need for action is imperative for areas of administration in which this is not already the case.

In the field of electronic delivery, §29, par.7 of the Service of Documents Act states that the service of documents must be carried out in a way that gives handicapped barrier-free access to the service using the current technology.

Survey of Barrier-free Access 2007

Between February and July 2007, as a result of an initiative between the Federal Chancellery and the Federal Ministries, a survey was carried out to determine the current status of barrier-free access to Web offerings on the federal level. The results of the survey have been compiled and are to be published in the Survey of Barrier-free Access 2007 (Erhebung Barrierefreiheit 2007)[65]. The survey offers an overview on the current situation and highlights areas for improvement.

On the basis of the survey results, concrete measures for the realisation of barrier-free access are being worked on and planned in individual ministries. The areas that need improvement include incorporating barrier-free access in future software developments and applications, as well as making improvements to existing solutions.

As a follow-up action, the ICT Strategy Unit has resolved to create a series of seminars on designing Web offerings with barrier-free

[65] http://www.digitales.oesterreich.gv.at/site/5715/default.aspx

access that are tailored to specific target groups and offer them to the Federal Academy for Public Services for people responsible for Web offerings in public administration.

Styleguide

eForms

The task of designing forms for public administration in Austria lies almost completely in the hands of the individual federal administration units. The goal is to offer the highest level of uniformity for electronic transactions in eGovernment and offer users an understandable and easy-to-use interface.

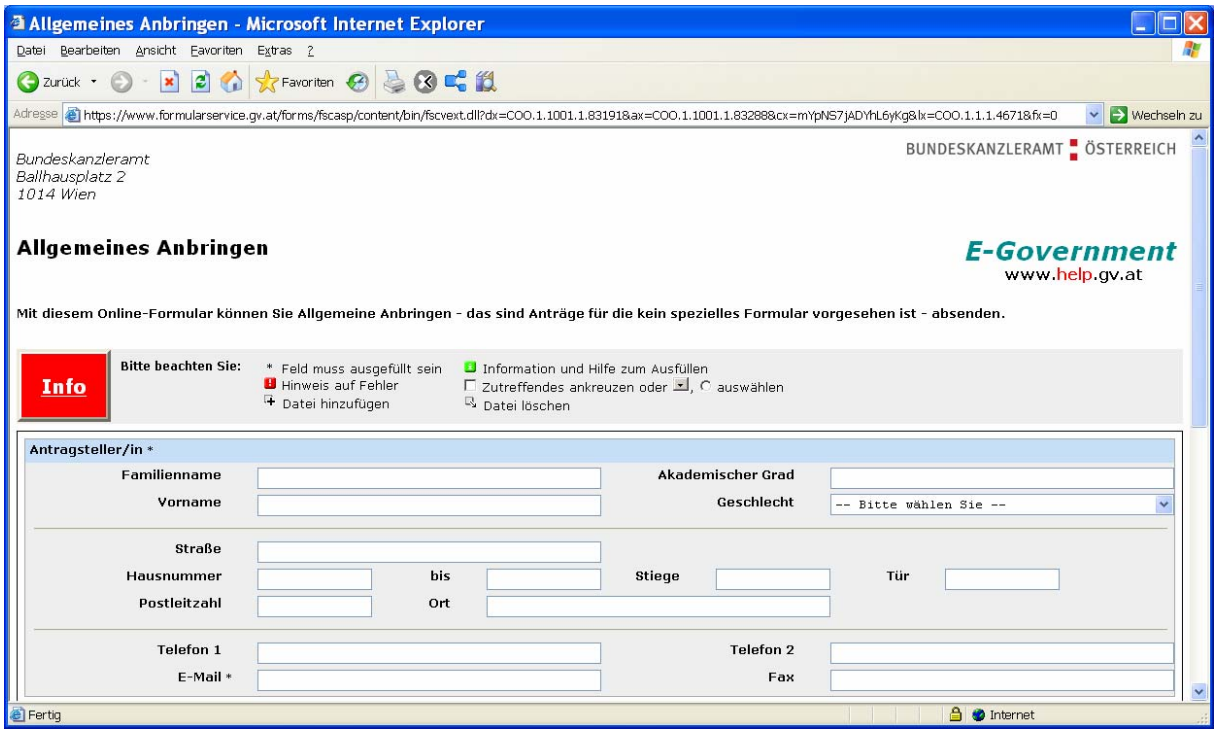


Figure 24: Online form design based on a styleguide

The styleguide for e-forms[66] (sg-stg) contains specific measures on structured design, systematic categorisation of content and visual design of online forms. Using a systematic, uniform and user-friendly approach to e-forms, it aims to simplify electronic transactions for citizens and businesses and make them as convenient as possible, to the benefit of both.

[66] http://www.ref.gv.at/Styleguide___stg_2_0_0_-_Versi.940.0.html

The specifications given in the styleguide have already been widely implemented and will play an important role in the development of other convenient functions like the cross-application use of user data (Data Only Once). These specifications still meet the requirements for protection of data across different areas because users keep full control over how their data is used.

Online Dialogs

The Conventions for Online Dialogs[67] (Konvention Online-Dialoge, sg-od) offers recommendations for creating applications using interactive online forms. It suggests individual steps for users on how to access the form, enter and change the information, and how to transmit the data to the proper administrative unit. The process should be uniform and recognizable across the administrative unit. Users should have access to applications that are simple and easy to understand. This helps to ensure that the electronic input is of high quality and error-free as possible so that the processing time can be reduced accordingly.

Communication Architecture

The Austrian eGovernment strategy requires active participation in creating interfaces that are standardised across public authorities and drafting specifications that are effective nationwide as part of the cooperation between the Federal Government, the provinces and municipalities. The results from the work groups are based wherever possible on international norms and standards, or use them as a model.

The typical eGovernment components that are needed in administrative and back-office processes join together to form a big picture, as shown in Figure 26. Along with individual applications, the big picture includes modules for online applications and components of the citizen card concept. The protocols used in the communication architecture function figuratively as the mortar which holds the building blocks together.

---

[67] http://www.ref.gv.at/Styleguide_Online_Dialoge__sg.722.0.html

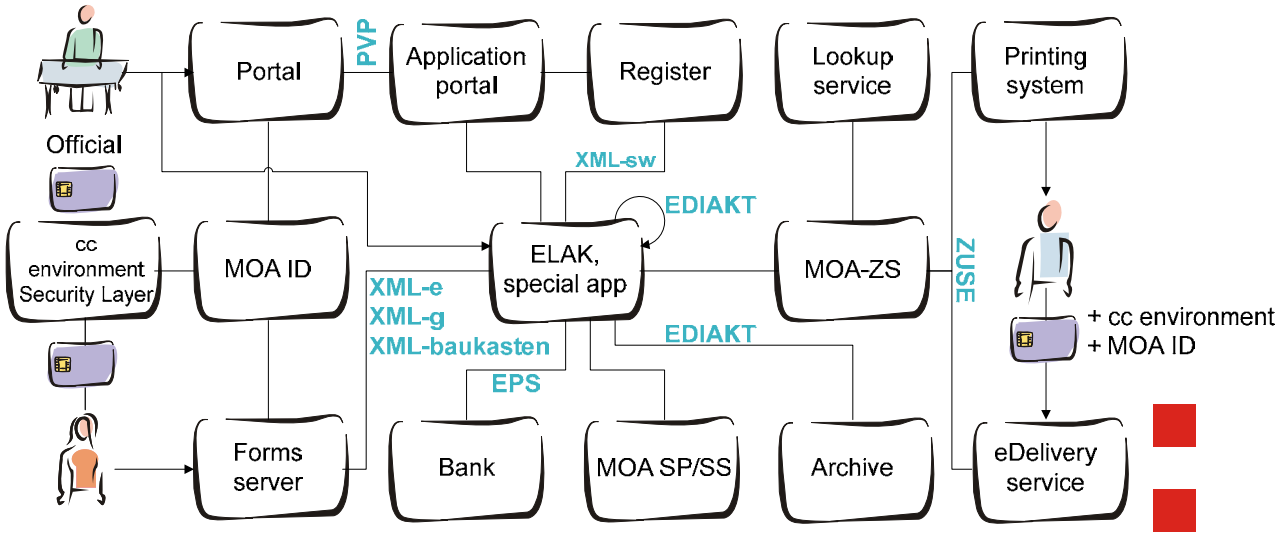


Figure 25: 'Big Picture' of eGovernment communication architecture

XML Data Input Protocol

Applications, notices, petitions and other data can be sent to the authorities from diverse systems using many different technical methods. Logging functions for tracking the input of this data into the record system must be made available. This is needed in order to record the successful transfer of data to the electronic input entry point so that confirmation messages can be sent back to the user's dialog window. The XML input protocol defines a standard for input data, regardless of whether it is sent from a public authority Web form or any other point. The entry point creates an XML data set which is stored on an ELAK or an archive system so that it can be processed by different applications when needed.

The XML input protocol forms the framework for all data which is used as input. This includes the actual data contained in an application form, any log data that is attached to it, as well as any additional data needed internally by the authority.

XML Structures for Business Objects

The XML business objects (XML-g) protocol contains a recommendation for a procedure that efficiently models XML structures for communicating between public authorities applications. The modelling recommendations are applicable to the creation of electronic application forms, amongst other things.

XML Toolbox

The XML toolbox describes a convention containing organisational and technical specifications for the design of XML data structures for electronic application forms. These should build upon the base elements and types, for which design requirements and the organisational expansion process are described.

Furthermore, recommendations for the use of base types and elements are specified in a separate schema. The elements and types defined in the XML toolbox for the input data element of the data input protocol are used in the implementation of electronic procedures.

XML Structure for Personal Data

The PersonData record is used to uniquely describe a person through interconnected information blocks called Person, Address and Signature. It is used in all eGovernment processes that handle personal data.

Applications that are built on this XML structure can further derive it, make restrictions or expand it as necessary to fit their own requirements. The top level generic Person object defines elements for both natural and legal persons. The elements that define a natural person include such aspects as names, alternative names (e.g., stage names), marital status, gender, place of birth, date of birth, citizenship, etc. The elements that describe a legal person include the full name, alternative names, the legal organisation form, etc.

The schema also includes a description for an abstract Address object with different specifications for telephone number, Web or postal address, along with elements specific to each attribute type.

Electronic Data Interchange Format (EDIAKT)

EDIAKT was developed as a format for standardising communication between different public institutions (authorities, courts of law, businesses). Although all had record management

systems that work with electronic records, business cases, and sub-cases including documents, the objects were specific to the manufacturer of the software and not built according to a uniform standard. In the course of further development of the EDIAKT system and due to increased distribution of the ELAK system, the standard was updated to its current format, EDIAKT II. Data is packaged as EDIAKT objects which are comprised of:

- meta-data that describes a record, business (sub-)case, or document
- process data for process instances and activities in accordance with the XPDL standard of the Workflow Management Coalition[68]
- content of the record, business (sub-)case, or document
- procedure-specific data that may be attached to an object

To satisfy the different requirements of institutions using ELAK, EDIAKT implemented a hierarchical structure with four layers. At the bottom is the document, which contains the file in its original format. If the file is not saved in a standard format, a document with a standard format must be attached.

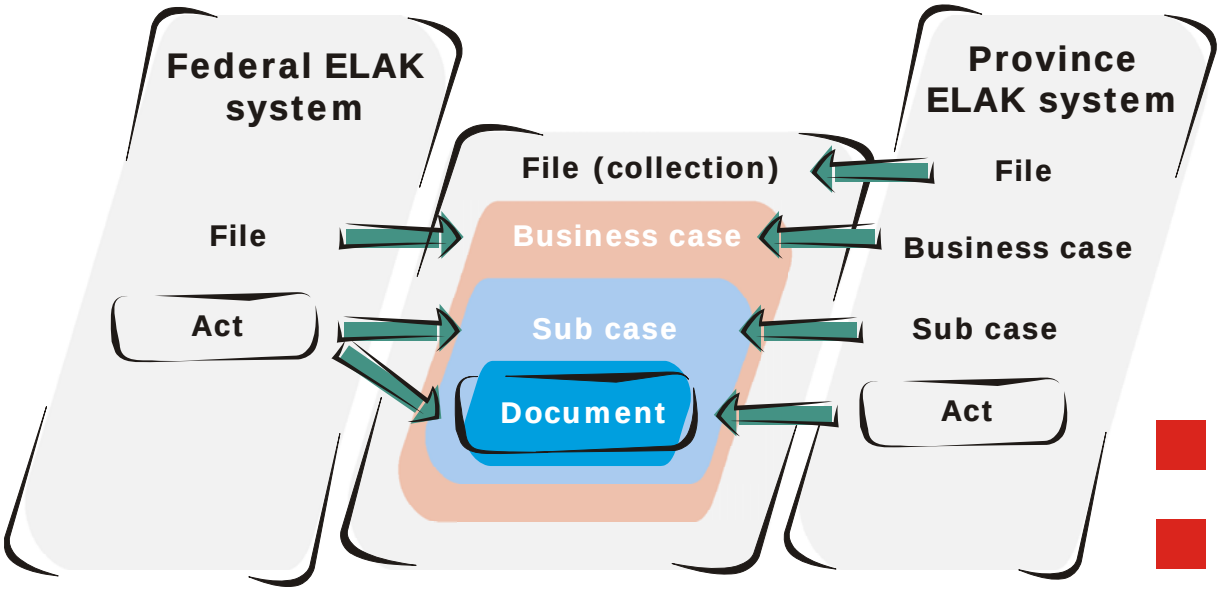


Figure 26: Structure of the EDIAKT format

[68] http://www.wfmc.org/standards/xpdl.htm

One or more documents are wrapped in a business sub-case. It represents the smallest object in EDIAKT II. This business sub-case may further be wrapped along with other sub-cases in a higher level business case.

Authorities that do not have their own ELAK system can still read EDIAKT packages using the free EDIAKT Viewer. The current version can be used to:

- display all meta-data including process data,
- show embedded documents and
- verify digital signatures.

EDIAKT is used more than just as an interface between different electronic record systems. It can also be used for internal data exchange between special applications and archive systems. EDIAKT II, together with the EDIAKT Viewer and EDIAKT Creator, and supplemented by the standard document format PDF/A, establishes the basis for the long-term archiving of records[69].

In the future, this format could play an increasingly central role for the submission of original records that is required for different courts of jurisdiction.

ELAK Transactions

EDIAKT created a uniform standard for the transmission of record information. The ELAK transaction convention takes it a step further and defines special information and electronic record management system functions and interfaces for the automated exchange of EDIAKT packages over Web services. This eliminates the need to export EDIAKT packages, save them temporarily and re-import them after they have been successfully transmitted.

Many administrations today are already working with electronic record management systems. Information systems that span all levels of administration, such as central registers, are gaining in popularity. The convention implements a standard that makes it

[69] http://www.bka.gv.at/site/5659/default.aspx

easier to couple diverse information systems together over a product-independent interface and to increase interoperability and integration of management systems. Data that may be used and is needed in administrative procedures can be integrated more efficiently into workflow processes.

The ELAK transaction specification is built on various base specifications of the ICT Strategy Unit. Its goal is the implementation of the following use cases:

- transmission of records, business cases and business sub-cases between ELAK systems.
- transmission of business case data from a central Branch Information System (Fachinformationssystem, or FIS) or from registers to decentralized ELAK systems where the actual handling of records takes places during indexing, duplication and transmission of business sub-cases.

Electronic Payments

Fees for public authority procedures are also applicable to digital services, and must be paid either during the procedure or afterwards. Fees can be paid by transferring the money over Internet banking. Additional methods that conform to uniform standards can also be integrated into the procedure such as credit card payments and mobile phone-based payment systems. The Electronic Payment Standard (EPS-2) is an open standard for synchronous online payments that was especially designed for payments via Internet banking systems. The EPS standard reduces implementation costs while increasing security at the same time.

The EPS-2 payment standard defines the communication process between an application and a payment system. It relies on XML notification messages, which are used to support the confirmation of payment. The bank communicates whether or not the payment was successful using an electronically signed payment receipt slip. It assumes responsibility for the actual entry of the payment in the ledger. It returns the confirmation message directly after the payment procedure has been carried out, even though the actual money has not been received yet. The advantage of this is that the confirmation message can be processed synchronously

further on in the process, (e.g., when an authority issues a notification right away, or when a handler arranges for delivery), or it can be archived as a receipt for verification purposes later.

The following steps are carried out for payments during online procedures:

1. The payment procedure is initiated by the applicant. The applicant selects a bank.
2. A payment request is sent to the bank that contains an XML message with a redirection URL that points to the eGovernment application. In response, the bank opens a session and forwards the user to the given URL.
3. The authority's application forwards the applicant on to the online banking application of his bank. After he has been authenticated, the payment transaction is carried out.
4. Before the transaction is carried out, the bank checks if there is still a connection open between the bank and the authority.
5. After the connection is confirmed by the authority, the bank carries out the money transfer.
6. A confirmation message is sent to the authority stating whether the payment was successful or not.
7. The authority responds with an acknowledgement message.
8. The payment process is finalised and the applicant is referred back to the authority's application.

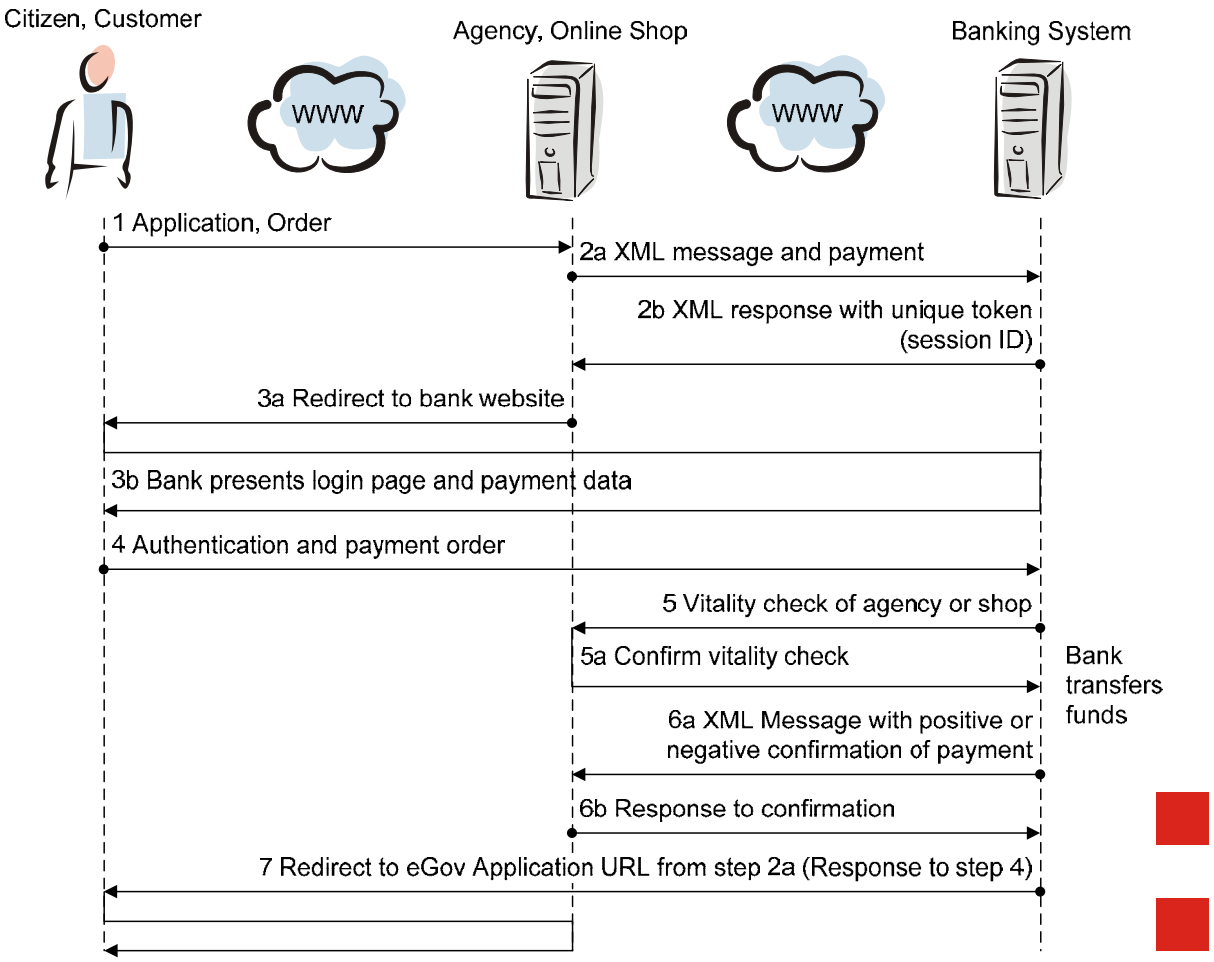


Figure 27: Process flow for electronic payments

Electronic Delivery

The main goal of electronic delivery is to replace paper-based communication between citizens and authorities as much as possible in the medium term. A large part of the outgoing communication from authorities requires proof that the document was only delivered to the intended recipient. This is done using RSa or RSb letters. In order to pick up a letter, the recipient must present valid identification to the deliverer, in this case, to the employee at the pick-up counter of the postal office. The receipt of delivery is sent back to the sender.

To confirm proof of delivery, electronic delivery relies on the citizen card's identification and authentication functionality to identify the recipient. In contrast to this method, proof of delivery for conventional e-mails cannot be verified and may therefore be contested.

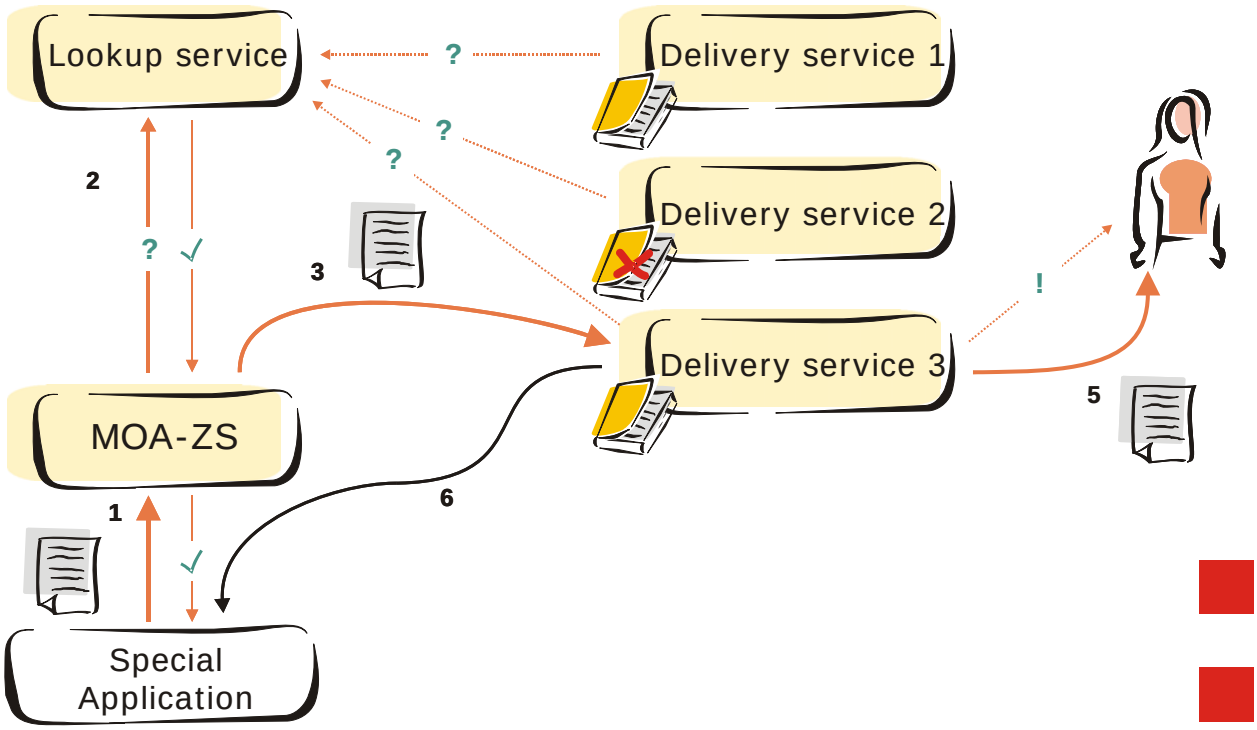


Figure 28: Process flow for electronic delivery

Procedures that allow automated pick-up are supported by law for cases in which automated acceptance of all deliveries has been configured, or when the use of the citizen card is difficult or less convenient. To set up an automated procedure for accepting deliveries, an agreement must first be made with the delivery service and the citizen card must be used when registering with the delivery service. The following steps are carried out when an authority wants to deliver a document:

1. The authority's application sends the document to be delivered to the MOA ZS. If necessary, it affixes an administrative signature and transmits the recipient's corresponding ssPIN.

2. A query is sent to the delivery agent to check which delivery service, if any, that the recipient has registered with, whether a hold on mail has been activated, and if an encryption certificate is available. If the recipient has registered his certificate with the delivery service, the document will be encrypted by the MOA ZS.

3. The MOA ZS transmits the document to the electronic delivery service that the recipient is registered with.

4. The citizen receives a notification from the delivery service that a document is waiting.

5. The citizen logs in to the delivery service using his citizen card, thereby signing the confirmation of delivery receipt for the delivered document.

6. The confirmation of delivery for the document is sent back to the authority, who then stores it, for example, in an electronic record.

MOA ZS automatically carries out all the necessary steps, including affixing the administrative signature whenever a piece of correspondence is sent to the MOA ZS. The steps which the MOA ZS should carry out can also be selected on an individual basis. For example, if the administrative signature was already affixed somewhere else, this step would no longer be necessary.

XML Search Queries

The XML specification for search queries (XML-sw) provides a standardised framework for the development of interfaces for searches, queries and information retrieval from eGovernment applications, such as registers.

This convention identifies two use cases: searching by attributes, which can return many hits, and searching using result recognition from previously saved searches that return exactly one result. It provides common XML elements for search queries in both use cases, a paging mechanism for queries that return large result sets, wildcard conventions, error codes and standards for creating new ones. This convention uses real register queries as a model for its implementation.

SOAP Faults

Keeping in line with the principles of the ICT Strategy Unit, the international open standard SOAP[70] is to be used for communication between eGovernment applications. Messages,

[70] Simple Object Access Protocol, http://www.w3c.org/soap

along with the corresponding information about transport, are transmitted in XML format using established Internet protocols such as HTTP or SMTP. With these types of connections, problems can occur which cause errors to be returned by the calling application. Protocols such as HTTP define error messages (e.g., 404 error: File not found) which are returned to the application. However, there are not any cross-application standardised error codes available for SOAP.

In general, the SOAP Faults[71] convention (XML-sf) recommends that public administration applications in Austria should return error codes. In development environments, error exceptions are thrown which must be caught accordingly. This ensures the standard handling of errors on the technical side for communication between Web service-oriented eGovernment applications. In addition, classes of error codes are defined to allow the source of the error to be quickly identified.

Diacritical Symbols

Diacritical symbols[72] are characters in the Latin alphabet A-Z that have had diacritical marks like umlauts, accents or ogonek added to them. This also includes special letters such as ligatures. Languages in the neighbouring European countries use more than 400 diacritical symbols. In Austria, the use of diacritical symbols is stipulated by law for civil registers, such as the central register.

In order to work with all the special characters in these languages at the same time, the Unicode character set standard[73] must be adopted. Unicode is recommended by the World Wide Web Consortium (W3C) as the encoding standard for Web applications on account of its secure future. It is also supported by all mainstream database systems, operation systems and programming languages.

---

[71] http://reference.E-Government.gv.at/Q-KA_XML-Soapfaults__xml-sf_1.634.0.html

[72] http://en.wikipedia.org/wiki/Diacritic

[73] http://en.wikipedia.org/wiki/Unicode

To ensure interoperability and avoid inconsistencies in data, all newly developed eGovernment applications should support Unicode. Applications which are not Unicode-capable should accept Unicode in the Web interface and convert it internally.

Infrastructure

ELAK

In their function as a document and workflow management system for the electronic implementation of internal work processes, electronic file systems (Elektronischer Akt, ELAK) become a kind of data hub in which different applications and data sources can be integrated so that changes in media format can be avoided. This is supported by a series of defined interfaces, through which an ELAK, as a core application of an authority, communicates with clients as well as other systems and applications.

In ELAK system of the federal administration, the most important interfaces and systems for public administration are:

- Form server: This interface displays forms in graphical user interfaces, making it the most important interface from the citizen's point of view. Application forms that are submitted over a Web form can be processed directly in the ELAK system due to their standardised data structure and XML syntax. The submitted application form is forwarded on to the responsible administrative unit for processing without delay.

- EPS 2 Interface: If any fees are incurred in the procedure, they can be paid by online banking, credit card or mobile phone, as described above. The standardised electronic payment confirmation is sent directly to the ELAK system of the authority and can be stored in an electronic record.

- Electronic delivery: In order to transmit information, notices, and documents to the intended person, the piece of correspondence must be delivered via a delivery service using the methods described.

- Interfaces to other applications: information is often needed from citizens during procedures which they are not able to supply, either because it would require too much effort, or because it may not be possible for the citizen to do so. Instead of citizens having to chase their data around, the data should be able to be accessed by the ELAK system in an automated manner from public administration applications such as registers, SAP systems or directory services. Communication occurs over defined interfaces that support the standardised exchange of data.

Portal Group

Within the portal group, data applications from one authority can be made accessible to other authorities on the basis of a common use and security agreement and a standardised portal group protocol (PVP)[74]. The portal group system allows participating organisations to use their own user management systems on the so-called base portal to access external applications. The operators of these applications can delegate the job of authenticating and authorising users to other portals. The operator defines access rights in accordance with the relevant statutory provisions for data protection. Access rights are granted to administrative units only, not to individual users. For individual users, roles are defined that users can be added to. Human resources grants access rights via roles to internal users according to their area of responsibility.

This has the advantages that it reduces the effort on the side of the application because it does not have to carry out user management. It also eliminates the need for multiple parallel user directories. In addition, single-sign-on is more convenient for users and makes the application easier to use.

Participation in the portal group is governed by the Portal Group Agreement. This agreement sets out the rights and duties with

[74] Registers that are accessible in the portal group include the Central Register of Residents, Register of Company Names, Central Commercial Register, and the Buildings and Homes Register (see http://www.ref.gv.at/Portalverbund.577.0.html).

which the joining partners must comply, such as carrying out user identification at login or other data security measures. Local authority bodies, public-law entities and other institutions performing public functions may also join the portal group.

The PVP forms the technical basis of the portal group. It supplements the organisational issues covered in the Portal Group Agreement (PVV) with technical details on the transmission of authentification and authorisation data. Other details include the protocol parameters, the link to HTTP or SOAP, the portal architecture, error messages and URL conventions. The portal group was built on the basis of existing technical foundations and has become very successful in the meantime. In the future, it will be necessary to normalise the protocol step by step to be in line with international standards so that it can be used as a basis for communication with other Member States.

Directory Services

Directory Services[75] serve as the infrastructure upon which various internal and external information services can be built. A central directory service and data model was developed for the Austrian Government for use on the LDAP.gv.at domain. The service has two functions. The first is to create a directory representing all the authorities in Austria. A country-wide address and telephone directory of public authorities will make them easier to be looked up and found. This increases the transparency of public administration. The directory supports a full-text search for authorities and enables navigation through the structure of organisations.

The second function has to do with the use of the directory service in the portal group. As previously explained, the authorisation process for accessing an application occurs over decentralised user management systems. These are implemented as directories on the portal. Base portals use LDAP.gv.at-conform directories in order to list employees as authorised users. Application portals, on the other hand, authorise administrative organisations according

[75] http://en.wikipedia.org/wiki/Directory_service

to their legal area of responsibility. The LDAP.gv.at specification defines a uniform data structure which comprises all portal-relevant information on organisations, organisational units, users, portals, applications and user rights.

Base and application portals must frequently exchange data and, due to the interoperable data models, are able to use the central directory service as a kind of data hub.

Registers and Special Applications

The difference between registers and special applications is that registers are created to fulfil a legal mandate. In many cases, the data in the registers must be made entirely or at least partly available to the public in accordance with legal regulations. Special applications, on the other hand, are primarily tools that make it easier for public administrations to carry out their legal mandates.

Today, registers and special applications are implemented as Web applications. More and more frequently, they contain Web service interfaces based on the SOAP protocol. To make cooperation in eGovernment projects easier, data structures were normalised for non application-specific cross-sector elements which were introduced in the communication architecture section. These elements are responsible for communication between authorities' applications, such as sending personal data, searching for information or returning error messages.

Registers and special applications require several lists that contain the same reference data, for example, academic grading scales or country codes. As part of the supporting infrastructure, an application for *central reference tables* is currently in development in which this type of data is maintained and distributed automatically. Having a central store will drastically reduce the amount of maintenance effort that, until now, had to be done by each individual application.

Modules for Online Applications

Modules for online applications (MOA) are software components that encapsulate all the procedures needed to carry out specific functions, as mandated by the eGovernment strategy. They also implement interfaces for Web applications. These modules make the intended functionality easier to integrate into applications. Some of the implemented functions include: verifying and affixing electronic signatures, reading identification data from the citizen card, and delivering notifications from authorities.

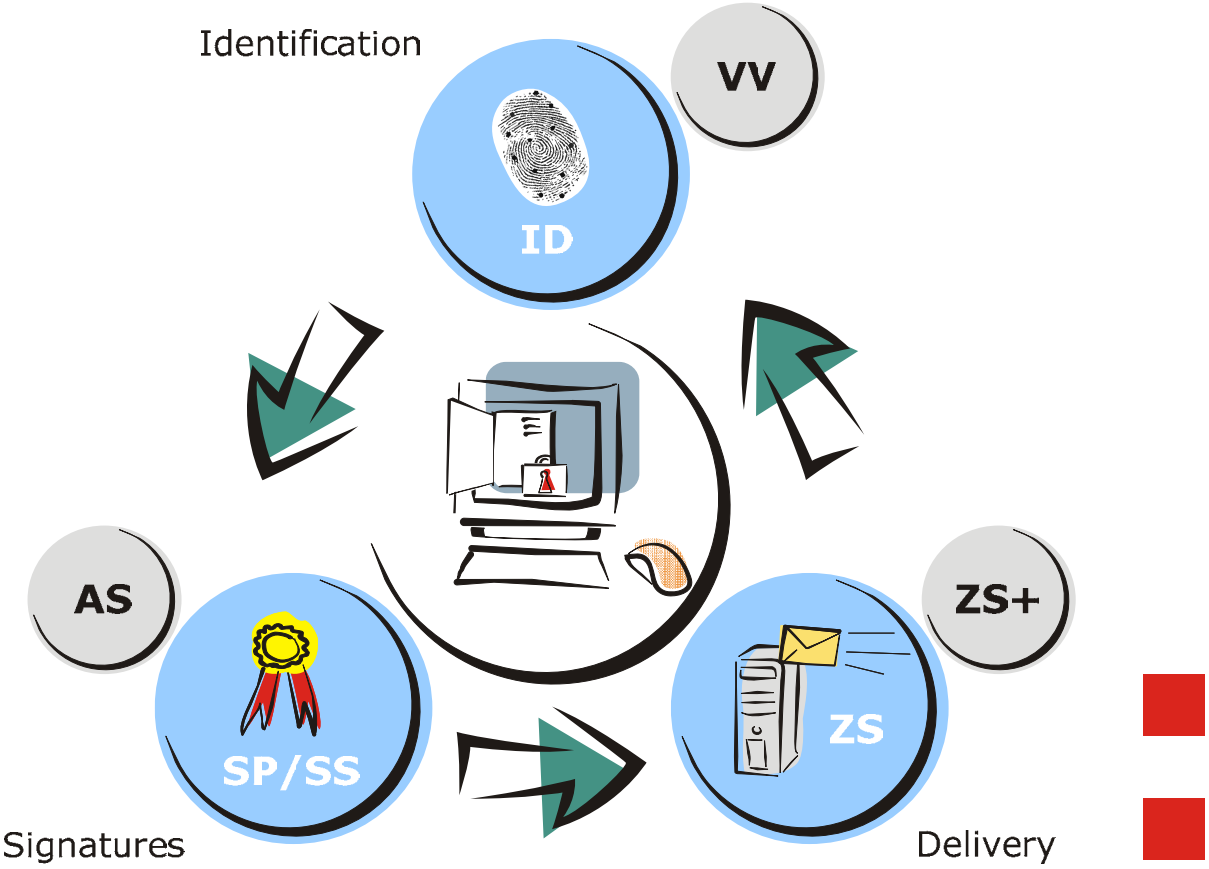


Figure 29: Overview of the modules for online applications

Right from the beginning, MOAs were conceptualised by the eGovernment Strategy for implementing interfaces on the basis of international open standards and for making licenses available for free. The fundamental specifications were published openly and since June 2005 the modules have been offered as open source software. This means that the source code can be looked at and further developed by anyone.

In the meantime, many eGovernment applications make use of MOA and its modules have become indispensable components of the system. For this reason, the software is continually maintained in a collaborative process and upgraded to fulfil new requirements. For this purpose, a platform[76] was created for the developer community so that feature and change requests, error reports and enhancements could be collaborated on in a structured way. The modules and all their versions including the source code are available on the platform. Currently, modules exist which support the following functionality:

- identification (MOA ID)
- signature verification (MOA SP)
- server-side signature creation (MOA SS)
- delivery (MOA ZS)

These modules are described in the following sections.

[76] http://www.egovlabs.gv.at

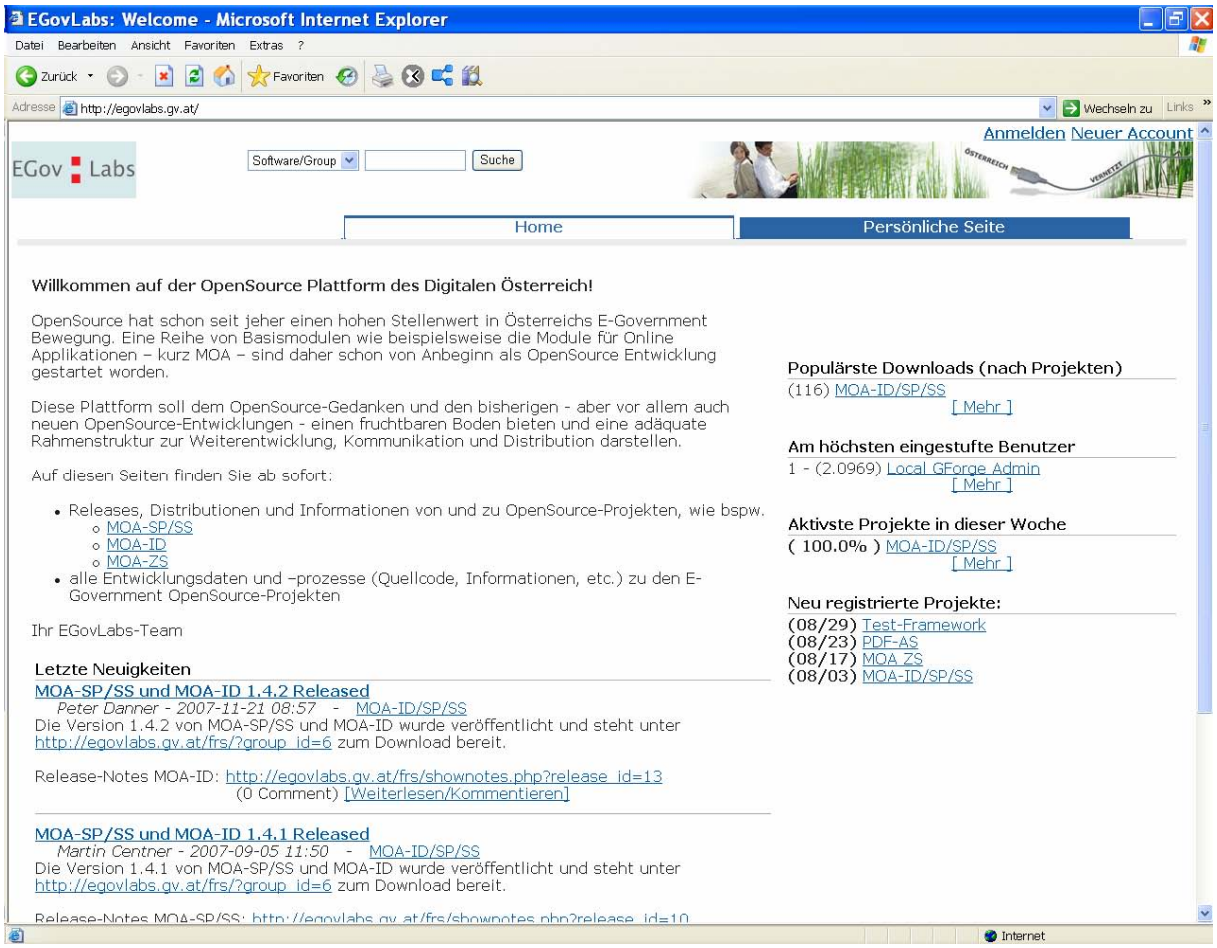


Figure 30: The open source platform eGovLabs

MOA ID

This module is used to uniquely identify and authenticate users securely who want to conduct online procedures with their citizen cards. The server-side MOA and the client-side citizen card software interact with each other to carry out identification and authentication using the identity link and the signature on the citizen card.

This logon process ensures the highest level of security for accessing records and accounts, carrying out bank transactions, and for all branches in which personal information and data is stored.

The MOA ID links a session to specific user data from the identity link, such as the sector-specific personal identifier, which the MOA ID calculates from the sourcePIN on the citizen card. The MOA ID includes functionality for accessing the citizen card environment,

communicating with the browser and citizen card environment, authenticating and identifying citizens, businesses and authorities using the digital signature and identity link, calculating the ssPIN and forwarding the user's login information to the subsequent application. The layout of the Web pages that are used in these processes can be changed to match the organisation's corporate design.

After authentication is successfully carried out, the application requests the login data from the MOA ID over a Web service or a Java interface. Alternately, a proxy component can be used to transmit the login data over other protocols (e.g., in a HTTP header parameter) for Web applications that do not support Web services or internal Java calls. This makes integrating authentification processes into existing online applications easy and uncomplicated. However, new eGovernment applications should be designed so that proxy components are no longer necessary.

Through the use of sector-specific personal identifiers in business applications, the eGovernment Act allows the citizen card to be used for identification purposes in the private sector. The upgraded features developed in the MOA WID project for the creation and use of sector-specific personal identifiers have been integrated into the newest version of the MOA ID.

Public authority procedures can also be carried out online by third-parties on someone else's behalf, as long as a valid electronic proxy authority agreement exists between the parties. The MOA VV was originally created for this purpose. It was able to authenticate electronic proxy agreements and recognize proxy limitations. The functionality of the MOA VV was also integrated into the MOA ID+.

For professional representatives (e.g., lawyers, civil engineers or administrative officials, who have authority to act in accordance with §5(3) E-GovG), the certificate extension[77] of the signature certificate in the citizen card shows that the representative is authorised to conduct electronic transactions on behalf of the principal. After the representative logs in with the citizen card, the

[77] See page 96

MOA ID is able to forward his identification data along with data of the principal to the application. In contrast to electronic proxy representation, where the data of the representative can be viewed in the XML structure of the proxy agreement, the principal is identified by entering attributes such as name, date of birth and place of birth on the login pages. The principal is identified over a Web service from the sourcePIN Authority, which sends his registration data (e.g., his ssPIN) back to the MOA ID. The MOA ID then sends the data on the subsequent application.

MOA SP/SS

This module encapsulates all functionality needed for server-side signature creation and verification. Signatures can be created using software certificates or with a hardware security module. The MOA module supports signatures according to XMLDSig[78] and CMS[79] for both signatures and qualified signatures. In order to create and verify signatures in the citizen card environment, the process and the XML-based query and response messages must conform to the citizen card specification.

During the creation of a signature, the module must look after obtaining the signature key, resolving of the data to be signed, calculating the transformation and creating the signature itself. It is also possible to create batch signatures with just one command that can be attached to many documents.

Just like in the MOA ID, its functions can be called by SOAP Web services as well as by Java program interfaces. The Web service interface makes it possible to maintain a clean separation between the calling applications and MOA components. In addition to providing the option for multitenancy, this design allows centralised modules to be shared by many applications.

[78] http://www.w3.org/TR/xmldsig-core/

[79] RFC 2630, http://www.ietf.org/rfc/rfc2630.txt

MOA ZS

The MOA ZS module creates the interface that is used between record delivery services and electronic file systems or special applications. It carries out a series of individual steps on its own, hidden from the user, that is necessary for the electronic transmission of tasks in a lawful and verifiable way.

With dual delivery, MOA ZA is responsible for communicating with the delivery agent, evaluating the method of delivery, affixing the administrative signature, encrypting the content of the electronic document (if required) and sending documents to a printing facility or an electronic delivery service. The confirmation of receipt from the delivery service to the authority is also sent back through the MOA ZA Web services.

This module saves application developers time and effort by implementing important basic steps in the electronic delivery procedure and thereby contributes to a rapid and cost-effective proliferation of electronic delivery. A trial implementation of it is already being carried out in the ELAKof the federal administration.

MOA AS

In order for authorities to make use of the popular PDF document format for electronic communication with citizens, an Official Signature must be able to be affixed to the PDF documents as specified in the eGovernment Act. According to §19 of the E-GovG, the document must be affixed with the Official Signature and the logo of the authority. MOA AS offers a simple Web service for attaching such signatures to PDF documents, which can still be reconstructed and validated even after being printed on paper.

MOA AS extends the functions of the signature module MOA SS/SP for attaching and validating PDF signatures. MOA SS/SP was specially developed for the signing of XML documents and therefore is not suitable for use as an Official Signature on its own. On the other hand, MOA AS makes it possible for eGovernment applications to add administrative signatures to common document types such as PDF, Microsoft Word or Open Document Format (ODF) so that they can be used for communication with citizens.

The specified PDF signature can be used for more than just communication by public administrations. It can also be put to use in the private sector as a simple way to sign orders and invoices electronically.

Summary

The institution-wide cooperation of all relevant decision makers within the Federal Platform Digital Austria contributes to the consolidation of existing structures and a clear distribution of competency in the implementation of eGovernment. The progress that has already been made in the implementation of administration-wide eGovernment services is the result of countless work groups working together to bring about a user-friendly eGovernment.

In the past few years, the basic fundamentals for a solid eGovernment were brought about by the realisation of numerous concepts, interface definitions, agreements on standards and technologies, new definitions of scope and the use of existing base components. The continuous development of additional components is made possible by the modular approach.

Concrete results from the ongoing realisation of eGovernment goals were able to be achieved since its start in 2001. Since the EU benchmarking of eGovernment services from two years ago, Austria has risen to the top of the list. Austrian eGovernment offerings were found not only to be comprehensive and extensive, they were also judged as being user-friendly and of the highest quality. It now remains to implement these fundamental elements across the board in order to stay competitive in the top field with other eGovernment countries.

:-)

SIMPLER. FASTER. BETTER.
THAT'S OFFICIAL.

FEDERAL CHANCELLERY ¦ AUSTRIA