e-government – e-citizen

Birgit Wilder

Chief Information Office Austria
A-1010 Vienna, Parkring 10/1/505
Birgit.Wilder@cio.gv.at

Abstract:
Living in the information society means radical change for all. New media and information and communication technologies are influencing our live more and more. At institutional level public adminstrations are subject to complete reorganisation following the new requirements of e-Government such as availability and comfort. Citizens are getting increasingly used to e-technolgies and the deployment of new media. Used to global information, e-commerce and quick responses from the internet e-citizens are demanding also from public adminstration higher efficiency, more transparency and better services. Comfort, availability and a homogeneous look and feel of applications will determine the acceptance of e-government. Austria has developed a nationwide approach to cope with the challenges of e-citizenship. This approach includes a high degree of security and data protection implemented by the concept "citizencard" and electronic signature at large scale.

The Austrian approach

e-government can be only successful if properly designed and accepted by citizens, companies and administrations. Therefore the Austrian strategy of e-government has been developed in cooperation with all relevant institutional players at national, regional and local level including the private sector.

Online applications will be better accepted and efficient if implemented homogeneously. The Austrian approach of e-government relies on a set of fundamental principles ensuring a consistent deployment of ICT in public administration:

1. Dual approach to avoid digital divide. Citizens can choose between electronic services or paper based transaction.
2. Encourage citizens to become e-citizens and use electronic services at their will.
3. Efficiency as common caracteristic of e-government independently at which level of administration offered.
4. Standardized processes and concepts guaranteeing security and privacy.
5. Coherent look and feel.
6. Transparency of administrative processes and procedures.
7. Interoperability of systems, applications and documents.
8. Open standards and freely available interface specifications.
9. Change management to allow the integration of future developments.
10. One stop shop concept enabling citizens to approach administration at a single point of contact without the need to know which adminstration is competent for what.

11. Back office reorganisation to optimize e-government.
12. Multichannel access to public online services. Technological neutral design is needed to allow citizens the choice of their preferred technology.

Structured e-government

e-goverment has to be comfortable and simple. This implies a standardized and well formed structure implemented uniformely by all administrations. Electronic signature, a well structured e-government access and standardized forms enable citizens to govern their own.

In Austria has been established the ICT-Board, a body at federal level responsible for a coordinated implementation of e-government. It cares for the collective use of infrastructure, the development of common policies and coherent procedures and the observation of adopted rules and standards.

The deployment of ICT can be seen as a chance for administrations to restructure back office processes and procedures leading to simplification and accelleration. The transition from paper based admininistration to e-government comprises a high potential of automatization. It remains only the necessity to interfere in the case of complex cases not following the rules mapped in the workflow. The time gained with automatization can be dedicated to better service.

Acceptance of e-government will raise if users encounter a uniform picture of public administration employing standardized procedures and forms. Currently numerous pilots, and prototype applications have been launched in Austria. Existing applications have to be adapted to the use of electronic signature. New applications are under way. Since the end of 2001 the Ministry of Public Administration together with the Ministry of Interior is developing a prototype of a complete electronic transaction with the use of the “citizencard” and the secure electronic signature. The first application available will be the criminal record.

The concept is based on following assumptions:

– *Modular design:*
Electronic transactions and processes can be seen as a set of basic components with clearly definded interfaces, functions and responsabilities.

– *System architecture:*
The communication between user and standard application is designed as follows: front end – portal – gateway – backoffice – delivery service.

– *Electronic signature*:
Citizens requests to administrative bodies are signed electronically. If legally necessary the secure electronic signature has to be used. To ensure legal certainty and authenticity server side signature of administrative bodies will be used.

– *Standards applied:*
Basic standards are TCP/IP, XML-format and XMLDsig. According to legal requirements

various security levels are forseen.

How e-government works

Open interfaces are pre-requisite of sucessful e-government. A smooth communication between user and application can only be achieved if specifications are defined in detail and made available to the public. Until now various XML-specifications have been defined in common effort with Länder (regions), municipalities, cities and the private sector.
Austria has build public accessible databases that offer specifications, interoperability conditions as well as other information and regulations relevant for e-government.
Formats on XML basis with formal description make possible the automatic processing of forms and the direct inclusion of electronic signatures in the document. When forms are designed properly they can be rebuilt from the screen or from a printout included the electronic signature. Forgery is impossible.
Authentic automatic reconstruction even from printout is crucial to cope with the various media and products in place.

XML-records specified for the implementation of e-government applications (www.cio.gv.at, http://reference.e-government.gv.at/):

1 XML-container
2 person data
3 electronically signed payment confirmation (in collaboration with banking institutes)
4 server side electronic signature (OID submitted to the Austrian Standards Institute)
5 delivery record
6 notification data
7 transmission data for online information

Work on the development of 4 basic modules is ongoing and will be finished at the end of this year.

4 basic modules:

? signature check
? authorization check
? identification
? server side signature

For the 25th October 2002 is planned a public event where the first prototypes and applications will be demonstrated to the public. Citizens and companies will be able to approach applications of public administrations electronically with the use of the electronic signature and the “citizencard”. Following applications are planned to be available:

? criminal record (Ministry of Interior)
? child allowance (Ministry for Social Affairs)

? paperless foreign trade administration (Ministry of Economy and Labour)
? request to residential registry (City of Vienna)
? tax declaration (Ministry of Finance)
? formless request (Federal Chancellery)
? issueing of “citizencard” (

The concept citizencard

In November 2000 the Austrian federal government decided to employ chip card technology to implement its intention layed down in the govermental programme to make available all public services electronically by the year 2005. By the year 2003 basic public services are foreseen to be accessible via Internet.

Security is one of the indispensible guiding principles for e-government ensuring legal certainty, identification and authentication. Today's state of the art are electronic signatures based on smart cards. But this doesn't mean that future technologies assuring requested security standards will be excluded of e-government. The principle of technology neutral design and well defined interfaces ensures a non discriminative approach and open markets.

Legal framework

With the reform of the administrative law[1] important steps have been taken to render possible e-government at legal level. To cope with the need for unequivocal identification and data protection the previsions for public adminstration procedures[2] has been modified introducing the derived and encrypted (one-way hash) public registration number. The adaptation of the delivery law[3] enables administration to deliver ufficial notifications electronically.

Concept citizencard

The connotation citizencard doesn't imply that the technology used must necessarily be a smart card. Equivalent alternative technologies are conceivable. At the time beeing the main instrument in Austria will be the smart card. The most important card because of its large scale use will be the social security card. There are various organisations planning to issue “citizencards” to there members or clients such as universities, the Chamber of Commerce, banks and the Austrian Computer Association. The introduction of service cards for civil servants is in consideration.

Smart cards which may be used for e-government have to comply with the requirements layed down in the concept citizencard (referred as “citizencard”):

1 Electronic signature functionality fulfilling the Austrian signature[4] law and the Austrian

[1] Verwaltungsreformgesetz 2001, BGBl. I Nr. 65/2002 (http://www.ris.bka.gv.at)
[2] Allgemeines Verwaltungsverfahrensgesetz, BGBl. Nr. 51/1991 idF BGBl. I Nr. 65/2002
[3] Zustellgesetz, BGBl. Nr. 200/1982 idF BGBl. I Nr. 65/2002
[4] Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), BGBl. I Nr. 190/1999 idF BGBl. I

signature order[5]. The law regulates identification and data origin authentication.

1 Secure electronic signature[6] which has the same legal effect as a handwritten signature.

1 A second key pair usable for peer entity authentication or for the set up of secure communication made possible by session certificates and session keys.

1 Info-boxes which can be used as containers for the storage of data such as certificates, identifiers with or without access control or any other data desired by the citiizencard owner.

1 Cryptografic binding of the ZMR[7]-number (each citizens resident in Austria is attributed a number in the central register) to a certificate. This binding is electronically signed by the Ministry of Interior competent for the central register of residents.

Security layer

An open interface called security layer, has been developed by public authorities. The security layer represents the mean which enables the communication between application and “citizencard”. The functions lying on the “citizencard” are capsuled in the “security capsule” and has to be provided by the industry. This enables the private sector to implement freely the citizencard. The advantage derived is the complete independancy between application and “citizencard” and the clear distinction of responsablities. The security layer meets the requirements of e-Government applications and ensures the market the possibility to join the citizencard project. Fully in line with the principle of open interfaces the security layer has been layed open to the public (www.buergerkarte.at).

The security layer is based on TCP/IP connections as communication channel and XML encoding for the communicated protocol elements. The use of TLS/HTTPS is also possible. SOAP and XML remote procedure calls (XML_RPS) are in consideration. The security layer uses a straight-forward request/ response protocol scheme. The application opens a connections to the capsule and sends its request. The caspule after having received the request, processes it, sends a repond and closes the connection.

Identification and Data Protection

Citizens approaching public administration electronically must have the certainty that their requests are not accessible to unauthorized persons and that they are clearly attributed to them. Identification by the use of electronic signature ensures these needs.

Nr. 32/2001

[5] Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), BGBl. II Nr. 30/2000

[6] The Austrian Signature Law uses the terminology “secure electronic signature” which corrisponds to the qualified electronic signature in the EU-Signature Directive.

[7] Central Registry of residents (Zentrales Melderegister)

It also facilitates citizens administrative contacts with authorities. No more prior registration is needed, no annoying User IDs and passwords are requested any more. The Austrian solution of the residence registry number (used in the central registry of residence) binded to a certificate makes it possible.

Data protection is a very important issue in Austria. To ensure confidentiality and data protection the above mentioned law regulating administrative procedures lays down that for the identification of persons the number attibuted in the central recidence register to each resident may not be stored by administrative bodies. The derived and encrypted (one-way hash) public registration number is a valid alternative. It ensures the reciprocal allocation of person and procedure respecting fully the requirement of confidentiality.