European Collaborative Innovation Centres for Broadband Media Service

JADE HOCHSCHULE Wilhelmshaven Oldenburg Elsfleth

Feasibility Study of an Open Source E-Government-Application

Case Study

EUROPEAN UNION
European Regional Development Fund

Investing in the future by working together for a sustainable and competitive region

The Interreg IVB North Sea Region Programme

Feasibility Study of an Open Source E-Government-Application

1 Contents

2 Executive Summary

It is currently very difficult to develop a European e-government system, which is valid for all countries. To different are the national requirements and the implementation of the relevant EU directives. However, the implementation of EU directives in Germany is so comprehensive that for most European countries the tool could be used but in individual cases this is to check.

The implementation of an e-government system includes a complete form server, a document management system, workflow system, a backup system and a full PKI implementation.

All these systems are necessary to complete verifiability of a document to ensure what is ultimately the basis for a conclusive e-government document. Only by clearly establishing who, when, what information, it can be a documented in a legal dispute as evidence to endure and this forms the basis of an e-government system.

Moreover, the requirement consists of the privacy that the transmitted data is only entrusted with the operation people / groups which will be made available. A blanket search of stored data must be made technically impossible. The evaluation process must not allow any conclusions about individuals.

3 Introduction

3.1 Sketch Project

The course of studies at a university from a student's point of view is made out of two significant aspects, which are increasingly supported by electronic means:

- Learning and teaching
- Study management

While the learning and teaching activities may easily be supported by mainstream tools like "Moodle" or other types of media, there are currently no broadband services available to facilitate the management of processes which are not directly related to learning and/or teaching. A university with campuses at different locations on the one hand, and a significant amount of students commuting between their homes and their campus on the other hand, could offer a much better quality of service by supporting its administrative processes over the internet.

Because the University of Applied Sciences in Wilhelmshaven is a governmental institution, it is bound by the appropriate public laws and regulations. The following communication scenarios regularly occur and have to be supported:

- Legally binding announcements of general information, such as exam terms and study requirements

- Legally binding announcements of information concerning a student's individual situation, such as ECTS certificates

- Processing of student's individual requests, such as acknowledgement of achievements from other universities or from abroad

- Observance of data privacy according to legal regulations

The project is aimed toward the development of a web based portal to support the study management according to the described scenarios. Initially, several cases are to be defined in order to demonstrate the typical interaction problems.

The further development preferably utilizes preexisting, general available software components. These will be extended on demand to meet the requirements posed by the e-government processes of a university.

3.2 Detail View (Concretization)

The following is a view of the situation at the university of applied sciences application scenarios.

3.2.1 Catchment Area

Present Study

The students of the university are mainly from the north-western part of Germany, but also from the rest of Germany and abroad. Especially students from the surrounding cities (50 km) hold no dwelling place of study, but commute from home to study.

Many students are located all over Germany and some in Europe for their internships and final semesters.

For organizational matters the students must not only keep the office hours, but often arrive solemnly for this very purpose.

The same applies to the employees of the university. Since the university has several study locations over a distance of 50 km, the employees / teachers are not living in the immediate vicinity.

Abbildung 1 Catchment Area

Online Courses

Yet for a much greater extent this relates to the students and teachers of the "virtual university", including the participating universities in Wilhelmshaven, Lübeck and Berlin, for the participants of the online courses.

Students travel from all over Germany and neighboring European countries to the presence of phases and tests. Organizational matters are done by email or postal mail, if legally binding agreements must be taken.

Abbildung 2 Distribution area online courses

4 Problem Statement

For an application, such as the one which is being investigated, a variety of Terms are to be clarified or differentiated. There are a number of laws, regulations and guidelines to be considered.

According to the research, a European-wide application (still) is not created because its true intent and framework exist at a European level, but national implementation or interpretation is very different.

Hence in this case study, only the German laws, regulations and policies will be considered. Where possible, references are made to the EU regulations. It is essential to verify the particular case of the national laws.

The German regulations are so comprehensive that the EU standards in some cases are exceeded, and the development of most provisions of the EU states will be met.

4.1.1 Terms and Definition

E-Government

For e-government (electronic government) the use of electronic information and communication technologies to integrate customer management in the actions of government and public administration is understood. The goal is to make the customers of administrative actions, as citizens, businesses and the administration itself, management services and information by electronic means. The potential uses of these technologies are very diverse. Beginning with the administrative modernization through electronic transaction processing, they extend beyond the provision of management information to authorities, Internet portals to the most complex transactions and interactive electronic services for citizens in the network.[1]

Legal Certainty

Legal certainty, according to the German view, is the clarity, certainty and stability in public decisions and the clarification of controversial legal issues or relationships in a reasonable time.

Court of Law

"Court of law" is not a term used in German law. The term implies however accountability and thus the legal security of organizations and processes.
In particular, any transaction by an instructional, evidentiary and documentation can be traced. This protects the individual employees and users in any event which may come.

Information Security

As information security is referred to properties of information and storing systems that ensure the confidentiality, availability and integrity. The information includes not only the security of IT systems and data stored but also the safety of not electronically processed information.

Confidentiality

1 Standards und Architekturen für E-Government-Anwendungen, SAGA Version 4.0, Bundesministerium des Inneren, 03/2008

Data may be read or modified by authorized users. This includes the access to stored data as well as during data transfer.

Integrity

Data may not be modified without detection. Respectively, all changes must be traceable.

Availability

To ensure the prevention of system failures, the access to data must be within an agreed timeframe.

Authenticity

Authenticity and credibility for a person or a service must be verifiable.

Document

A document, in the sense of this document, describes uniformly stored electronic data.
A document can consist of one or more components. It can have uniform or differentiated access. A document can be signed in whole or in part. A document is always clearly comprehensible and must be able to be reconstructed at any time.

Document Management System

Computerized system for storage and processing of "documents" in electronic form.

Workflow

A workflow is a predefined sequence of activities in an organization. A workflow is a closed content, time and factually logical sequence of continuous functions that are necessary for the processing of a relevant object. Each instance in this sequence may be assigned to a certain actor (person) or a particular resource (DV function).

4.1.2 Statutory Provisions

The following laws (at least in parts) must be observed:

BGB (German Civil Code)

The Civil Code provides in § 126a the principle that any document, unless another form is prescribed, can also be submitted as an electronic document when a qualified electronic signature is available. Thus the qualified electronic signature of the signature is made equal.

VwVfG (Administrative Procedure Law) [2]

The Administrative Procedure Law governs the principle of administrative processes between public institutions and citizens. Two paragraphs have noted particular attention:
Electronic communication
§ 3.2 paragraph 2 explains explicitly the signing of documents submitted with a qualified electronic signature according to the Signature Act. § 3.3 clearly indicates that each document on request in another format or as electronic document must be made available to the recipient
Determination and the form of an administrative act

[2] VwVfG vom 25.05.1976

§ 37, 3 notes that documents submitted by the institution must always be signed and show the certificate. The institution must be remitted.

SigG (Signature Act)

The Signature Act regulates the term of the qualified electronic signature, and whose production, management, and partly to their use. It is an implementation of EC law EGRL 34/98 and EU Directive 1999/93/EC.

The § 23 explicitly regulates the use of foreign electronic signatures and the products for electronic signatures as implementing Article 5 of Directive 1999/93/EC. The use of foreign domestic signatures signatures equal footing.

SigV (Signature Regulation)

The SigV regulates the requirements for components of the production and use of electronic signatures. § 15, 2 regulates the signature application components.
§ 17 explains to the process for long-term backup. It should be noted that the data must be kept longer than the current validity of the signature when it needs to be re-signed. The re-signing includes the whole document, complete with original signature and needs to be done before the original signature is invalid.

BDSG (German Data Protection Act)

The Federal Data Protection Act governs the general handling of data. A special attention has to this investigation, the second section which regulates (§ 12-26) the "Data processing at public authorities". Such state owned data protection laws (e.g. NDSG) shall apply accordingly.
In essence data economy, security, storage, and use of Changes are regulated.

4.1.3 Recommendations

The German Federal Government has established a number of recommendations and standards that must be considered in the development of e-government applications. These are not mandatory. However, it is advisable to know and to observe these in parts.

SAGA 4.0 (Standards and Architectures for e-government applications)

The objective of this document aims at primarily interoperability, reusability, openness, reduction of costs and risks, and the scalability of e-government applications. To achieve these objectives SAGA is used for a number of recommendations on architecture, infrastructure, and to use standards and technologies in e-government projects in public administrations.

DOMEA (Document management and electronic filing in the IT-enabled business course)

The main objective of the DOMEA concept is the introduction of the electronic file. Because the same laws, rules, guidelines and rules for paper files applz, official business, transaction processing and archiving must be transferred to fully compliant IT processes. DOMEA will supply guidelines.
After DOMEA developed products can be certified.

MoReq2010 (Model Requirements for the Management of Electronic Documents and Records)

Is the equivalent to DOMEA of the European Union. MoReq was originally created for data exchanges between the EU states but has been extended and finds its implementation in national recommendations.

NPSI (National Plan for Information Infrastructure Protection)
It accommodates recommendations for the protection of the IT structures.

XÖV (XML standards in public administration)
XÖV called technical standards for electronic data exchange in the public service is based on standards to enable seamless XML. These standards will enable seamless electronic business processes in public administrations in Germany.

ISO 19005-1 / PDF-A
Is a pseudo standard for long-term archiving as PDF documents. The technical standards contain many references to the implementation of the XML structures.

5 Requirements

The legal requirements and recommendations named in the section "Problem Statement", produce quite a number of basic requirements for an e-government system which will be complemented by requirements of the institution.

5.1 Global Requirements

A System is to be created which has very low entry thresholds. For this reason, a default web server should be able to process the e-government application.

In order to avoid licensing costs only open-source products are used. Only one SSL certificate that is mandatory would produce costs.
Because of the components which are used each administrator should in a position to set up an e-government application.

This has the following basic requirements:

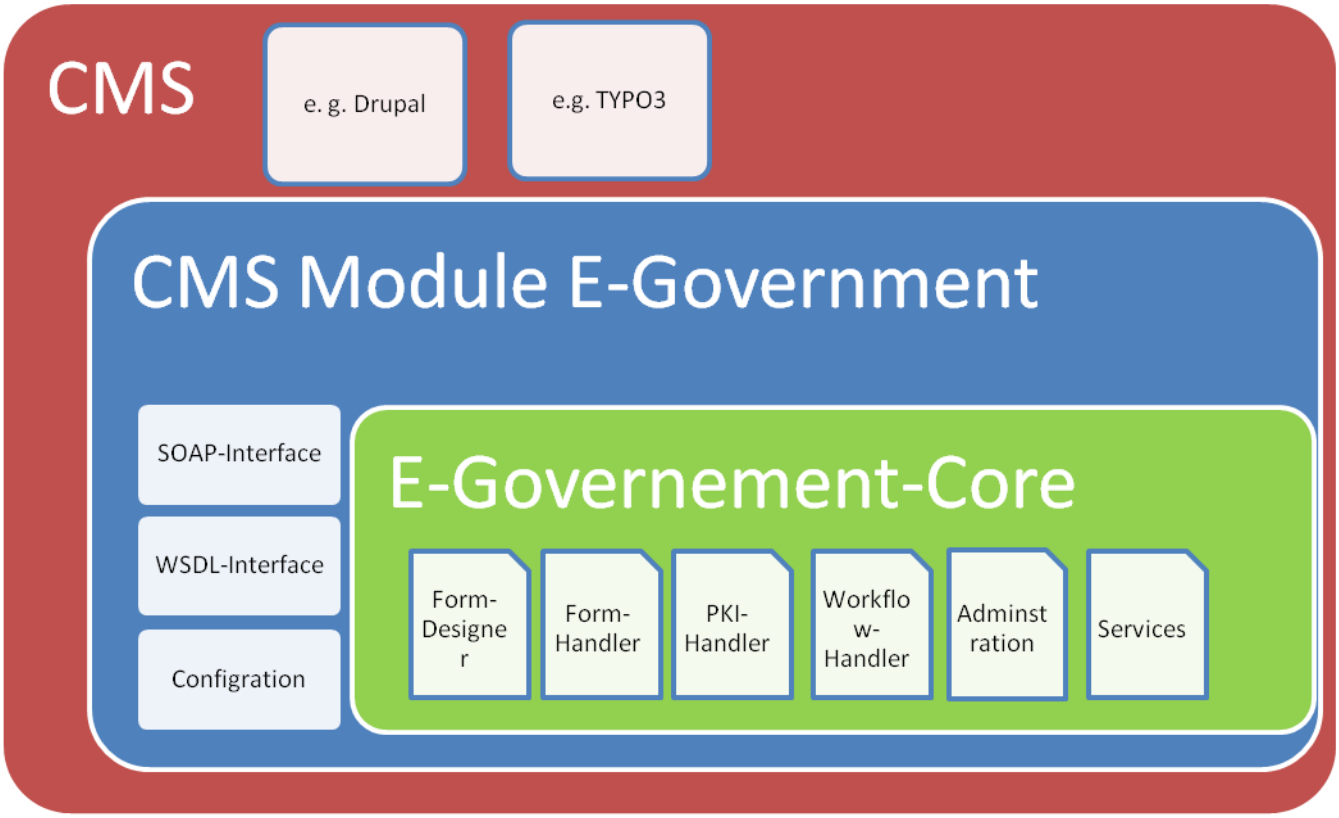
- Linux Operating System
- Apache-Webserver
- PHP 5.x
- MySQL 5.x
- Object orientation
- Modular design
- Accomplish in Firefox 3.x, IE 7.x, Safari
- Usable in different CMS
- Low learning curve

5.2 Requirements of the CMS

Differentiated user access rights
Multilingual
Barrier free / arm

5.3 The system to be Developed

The system should be equipped with a modular core which can represent all the features. The core is then integrated into a module of the respective CMS. The configuration is then carried in a CMS module. In this way, the e-government tool can be integrated into any CMS and the user can use familiar CMS.



The core contains modules that represent the desired functions. Depending on which version the core is being developed with, the required modules to be added to the core.

5.3.1 Variant A

Form put online

1. With the Form Designer the form is created. The Form Designer can also establish the release of the publishing times or unpublishing times. Here the archiving period must also be set to 1, 2, 3, 5 or 10 years.

2. The form handler assigns the form of rights group and saves the form in the version management. Over an interface forms / documents from trusted sites (applications) are uploaded in whole or in part (for example, option-lists generated documents).

3. The specific access permissions and workflow settings can now be defined.

4. The form handler clears the form. The form / document can now be provided with a standard or specific signature, so that each user can see the inquiring agency.

5. Now the form is ready for the digital signature using a simple URL (e.g.: https: / / <EGov-Server> / <FormName>. Html) and is available to every user who has access to this address who provide the digital signature.

Digitally signing a Form

1. The user loads over an encrypted connection, the form / document in his Internet browser. Depending on the workflow setting, the form / document is here already assigned to a meta-document.

2. The user fills in fields at the screen, or reads the document.

3. To start the signature process, the user presses a button at the end of the completed form or document. Thus its input data will be transferred to the form handler.

4. The form handler performs the validation and after successful validation the hash module generates a unique name and a hash value for the document. This data is appended to the document. Only then the form handler releases the signature applet.

5. In the signature applet the data is displayed again and signed.

    a. If the user starts the signing applet for the first time it is automatically searched for a signature card and a card reader.

6. The user signs the form / document in the signature applet with its inputs. The user has the option to print or save this document locally with his signature.

7. The form handler saves the signed document in the document archive. Automatically the integrity of the signed document will ensure the digital signature and queried the validity of the signature certificate in the Trust Center.
   Alternatively, the user can save the document without a signature and complete the signature on record to a trusted authority. The stored data will not be disclosed until the full signing in the workflow has been completed.
   A user can view his own hand-signed documents over a particular portal or call a special document on the document name.

8. Lastly, the user receives a confirmation message concerning the proper registration to the digitally signed form / document.

    a. If the document is flawed and its data is faulty, for example in the manual follow-up, the document or the document part is invalid and must be generated again.

Interfaces

A document adopted generally triggers a workflow.
In the simplest case, an agent will be notified by mail about the reception of a document. The

application can also be a function of another trusted application access and transfer the data or pieces of data.
A Web interface allows the authorized agent to access all relevant documents, or documents to trigger workflows to be exported. Trusted applications are subjected to an interface available to retrieve documents or document parts.

An agent has the opportunity to declare a document or document part to be defective. This part may be subsequently created again and will be excluded from the export.

Another interface is a backup interface, which is protected separately, because the data in clear text for permanent storage can be exported. The archiving is done in XML.

Data Export

By default, XML, or CSV formats are supported for export.

Cron-Jobs

The application requires a continuous cron job which monitors und runs the releases, backups and workflows.

5.3.2 Variant B

Variant B differs from variant A in the manner of implementation of the forms.
This can be specified on the ACTION tag in the HTML form of the eGov-server. The form is forwarded to the server when send to the eGov-server. Previously however, the validation should be done.

Solemnly the first step of the variant A is left out.

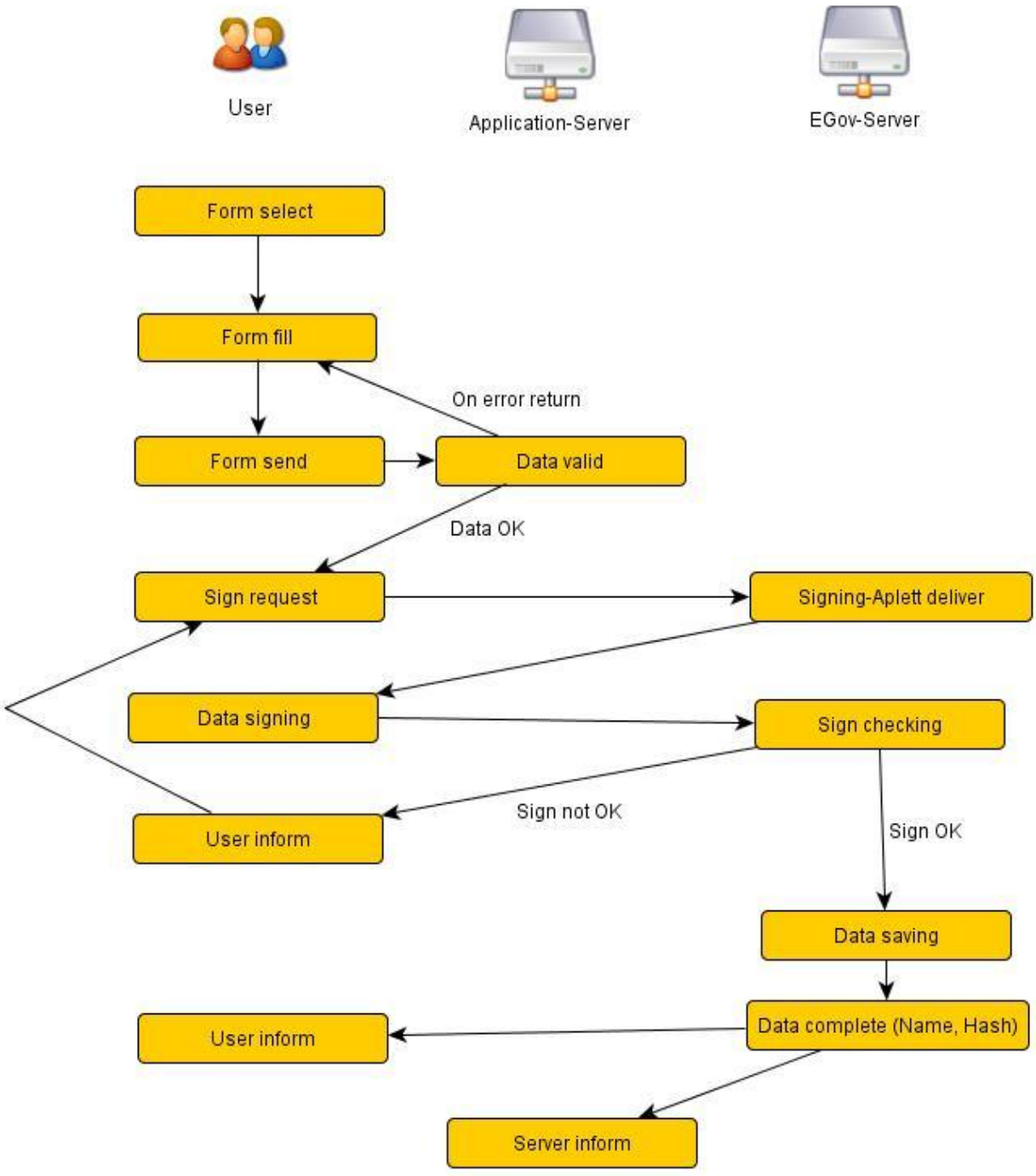


Abbildung 3: Activity Variant B

Important in this version is that the communication is always held directly between the user and the appropriate server.

A disadvantage of the variant B is a certain loss of control at the access level and the availability form. However, the implementation a form designer in the eGov-server is left out.

5.4 The Core-Module

Not all core modules can be distinguished clearly. Thus belongs, e.g. to the form design also the creation of the corresponding workflows, or vice versa, depending on the starting point.
In principle however, all functions are mapped without redundancies. Some features are of the same name here but are from different contents. So there is a version control for the overall system but also a separate version control for forms but they have fundamentally different tasks.

5.4.1 Administration

The administration module handles all global settings and configurations:

- Creating users with access to create workflows.
- Integration of LDAP groups.
- Setting up roles.
- Setting up languages.
- Evaluation of statistics.
- Evaluation of protocols.
- Definition of alert levels and events.
- Creating and verifying backups.
- Setting up archiving periods.
- Deleting any unnecessary data.
- Version Control
- Creating and managing positive and negative lists for users

This is to ensure that the function is made available to only particularly trustworthy, educated and trained personnel. This is because by the backups a direct access to the stored data would be possible.

5.4.2 Form-Designer

The Form-Designer will create forms and workflows for individuals or groups of persons entitled to process and manage these. On the forms and the evaluation of the form contents have been received only for certain individuals or groups can access.

Forms in this sense are all the documents required in the e-government tool. A signing, including text (messages), images, files of which notification must be recorded are binding.

Each form is given a unique name, link and a version number. From the name and version number, the application ID is formed, which is always stored with the data transmitted.
When you call the forms always the last active version of a form is delivered. All old versions are

maintained or not activated in version control to create it if necessary sent forms with the submitted content again.

All of the forms will be provided with publication dates (from / until). The accessing of persons can be restricted (by positive or negative lists, such as IP subnet, IP address exclusion, group membership). Maximum document sizes can be determined. It can be queried data for process monitoring.
In all cases, retention periods should be established.

In principle, the following form elements can be created in the first version:

- Textfield
- Textarea
- Checkbox
- Checkbox-Group
- Radio-Button
- Radio-Button-Group
- Select-Box
- Date-Fields
- Static Text
- Files (File-Upload)
- Fieldset
- Images

For all the form elements CSS attributes, Post- or prefix can be defined.

For identified form-users the first eight elements with default values via a special service function can be assigned and the checkbox or radio button group can form the elements of on-demand via a special function. For this, a common identifier (such as LDAP name, student number) or another key to a service function is provided and puts the data in XML or JSON, contrary reviewed and incorporated into the item before delivery.
In this way, for example, a test application for a student using the student number from the service function of the higher education information system (HIS) a list of courses available will be created.

For all data to be transmitted validation rules can be defined. It sets a series of simple validations if it is empty, numeric, is an email address, and has a minimum length of the input and so on. Alternatively, services or code sequences are to be entered for validation.

For the export or backup of the forms a special XML format is used, see chapter „6 Database Design and export formats”.

5.4.3 Form-Handler

The form handler has two major tasks.

1. It collects the data and must ensure the following:
    - Provide Form.
        - It prepares the forms before delivery,
        - delivers forms,
        - takes the data received,
        - validates the data submitted,
        - gives it back if necessary,
        - assigns a unique name,
        - assigns a unique hash,
        - saves the data and
        - starts the signing.

2. After the data is collected and stored it must be possible to replicate this at any time to confirm the authenticity of the data or to compare one document to another. There is a web interface in which the unique name of a stored document, the original document, of eligible persons to retrieve the document again or to be compared it to another document. This requires that the form handler must be able to:

    - Restore forms,
        - can check the hash of a document,
        - can compare or create a hash for a different document,
        - recheck a timestamp,
        - expand documents with signatures

The procedure how the hash is created allows to say whether a binding document was tampered with or whether two documents are identical and thus to prove the authenticity of a document.

A further task is to prepare documents for a backup. Documents are to be stored for up to 30 years. Because of this a simple database backup is not enough, so the documents are secured in a special XML format in plain text. See “6 Database Design and export formats”. Only in this way the safe recovery of each document is ensured.

5.4.4 PKI-Handler

The PKI handler contains all the functions to detect the "signatures", the review, their storage, their restoration and protection.

The PKI handler uses various methods, such as an integrated Java applet, a browser interface (which is planned for the next versions of Firefox and Internet Explorer) or a defined external program, such as the citizen-client of the German Federal Government.

5.4.5 Workflow-Handler

The workflow handler monitors the various events that were set when the form is designed. If an event has occurred, for example, data sent and stored, is reviewed by th workflow handler if further steps are necessary. For example, the data will be forwarded to different people / agencies for further processing.

Provided is:

- forwarding by email to one or more persons / agency different events
- forwarding via SOAP / WSDL to defined, reliable systems for additional processing of the data
- Delete any unnecessary data.
- Error analysis and notification of outages for administrators.

It can also be created from eligible persons / groups, process monitoring (e.g. lead times). This is to ensure that the privacy provisions that prohibit the monitoring of individuals are respected. It can thus only analyze the overall processes of all stored cases and cannot be used for individual monitoring are.

5.4.6 Services

Among services, all functions are taken, that the system uses for other modules. Here are located the system interfaces SOAP, WSDL, XML, etc.

There are some special functions to call:

- Time Stamp function, either a radio controlled clock or a specific timestamp server (for example, the DFN)
- Mail-Function
- Encryption and Decryption
- Database-Wrapper
- XML-Function

6 Database-Design and Export-Format

The database design is kept very simple:

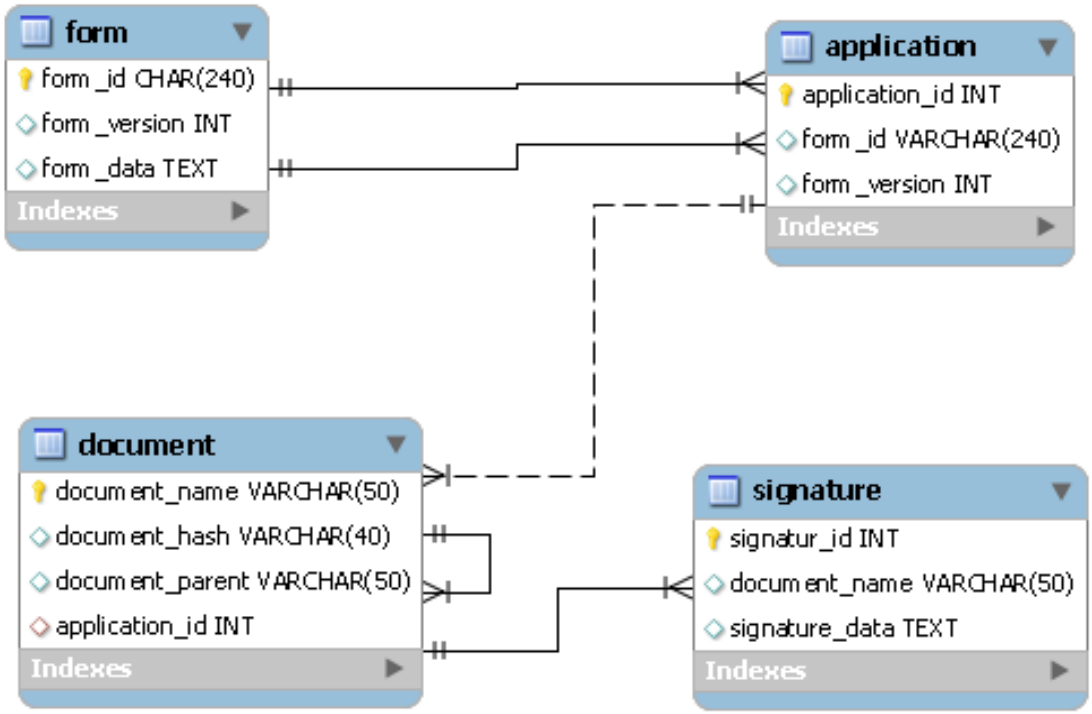


Abbildung 4 Database-Basis-Layout

To see here are only the logical relationships between the tables of the database needed to store the documents. For purposes of simplification, the users, owners and their rights are not shown.

Basically, this design allows storing of any number of forms and their variants. From the form_id and form_version the application_id is produced. The application_id is refrenced to a document for the appropriate form. It can store any number of documents. The signature is always related to a specific document (document_name). It allows any number of signatures appended to a document. Each document can stand by itself or refer to another document (document_parent). The child document can refer to any application_id. A root document can have any number of child documents and all child documents have the same characteristics (skills) as a root document, such as one's own rights in turn, allocate or any number of child documents.

With this structure, complex trees can be built that can represent any process.

In the same way XML documents are generated. The full data and XML declaration is beyond the scope of this Case Study and will be processed in a further case study.