SU eServices

Final report

Developed by:

 Sentido Ltd.

 Boris Chervenkov

 boris.chervenkov@sentido.bg

 CITA Ltd.

 Svetlin Nakov

 svetlin.nakov@citagency.eu

September 2012

Table of contents

Sofia University – short presentation 4

Sentido – short presentation 8

Experience and technologies 8

Contacts 9

Major projects 9

CITA – short presentation 11

Mission and vision 11

Areas of Expertise 12

Project overview and scope 13

Student’s certificate request 13

Students’s GPA reports 14

Science projects 14

Project management – approach and methodologies 16

Inception phase 16

Elaboration phase 17

Construction phase 19

Transition phase 20

Training 21

Conformance with Bulgaria’s e-Government 22

Technology overview 24

Database – goals and design 24

Deployment environment 27

User Interface and design 27

Portal user interface design 27

Backend user interface design 28

User management, authentication and access rights 28

Security and threat management 29

Approach to security architecture 30

Security strategies 32

# Sofia University – short presentation

The University is the first school of higher education in Bulgaria.

Its history is an embodiment and a continuation of centuries of cultural and educational tradition in this country.

Explore the largest and most prestigious educational and scientific centre offering 99 degree courses in humanities and sciences via our Web Site.

Sofia University St. Kliment Ohridski is the first institution of higher education in Bulgaria. The first step towards its foundation was the opening of a Course in Pedagogy at the First Secondary School for Boys in Sofia in 1887. Due to the success of this teacher-training course,the National Assembly issued a decree at the end of 1888, transforming the course into a School of Higher Education. In 1904 a decree by Prince Ferdinand turned it into a university that was given the name of St. Kliment Ohridski a year later.

For more than a century Sofia University has been the national foremost centre for university education and research in both fundamental theoretical and applied areas. Today it is the largest university in the country with 88 degree programmes offered by 16 faculties.

The first building of Sofia University was erected thanks to the donation of the brothers Evlogy and Christo Georgiev and today ranks among the most interesting buildings of the architectural heritage of Sofia. It spreads over a total of 36000 sq. metres and has 324 rooms, including 65 auditoriums with a total of 6000 seats.

Sofia University comprises: Faculty of Slavic Studies, Faculty of Classical and Modern Philology, Faculty of History, Faculty of Philosophy, Faculty of Law, Faculty of Journalism and Mass Communication, Faculty of Education, Faculty of Preschool and Primary School Education, Faculty of Geology and Geography, Faculty of Physics, Faculty of Mathematics and Informatics, the Faculty of Chemistry, the Faculty of Biology, Faculty of Economics and Business Administration, Faculty of Theology, Faculty of Medicine, Department of Information and In-service Teacher Training, Department of Language Learning, Department of Sport, Germanikum Institute for German Studies, National Lyceum for Ancient Languages and Cultures St. Constantine-Cyril Philosopher, National Lyceum for Mathematics and Natural Science L. Chakalov.

A total of 25368 students have enrolled at Sofia University for the 2006/2007 academic year. 17511 of them enrolled at the Bachelor’s Programmes (16418 Bulgarian and 1093 international students) and 7857 students enrolled at the Master’s Programmes at Sofia University (7638 Bulgarian and 219 international students). There are 969 PhD students of whom 832 Bulgarian and 137 international.

The teaching staff includes a significant part of the best specialists in Bulgaria in all major areas of sciences and humanities. There are 1598 full-time lecturers employed. These are 2 Members and 4 corresponding Members of the Bulgarian Academy of Sciences, 192 professors, 594 associate professors, 809 assistant professors, 2 senior research fellows and 1 lecturer. 209 of them have the higher doctoral degree of Dr. Habil. and 928 have a PhD degree.

Research is an integral part of the teaching process. It is fully supported yet not conducted by the Rector’s administration. Research is a prerequisite for keeping pace with the most recent developments in the respective areas for both the lecturers and university structures – laboratories, faculties, etc. The following figures (indicative for the period from 2001 to 2005) testify to intensive scientific development and integration between research and teaching practices:

* the research papers of various fields increased three times;
* number of conference and symposium participations in Bulgaria – more than 3638;
* number of conference and symposium participations abroad – more than 3579;
* number of publications:
	+ monographs – 712;
	+ textbooks, anthologies and readers, and reference materials – more than 1821;
	+ published papers, articles, and reviews – over 10 385;
* hundreds of ongoing joint international projects.

International relations have a special place in the University’s global strategy as they considerably stimulate research, and support and improve the quality of teaching. Sofia University has contracts with more than 80 universities of different countries, thus facilitating a wide variety of joint international projects and multilateral professional contacts with colleagues from all over the world.

During the academic 1999/2000 the University signed a contract to join the Socrates Programme of the European Commission. It has since held a leading position among universities in the country, with the highest rate of student and staff mobilities and the most significant contribution to the maintenance of European standards in higher education.

# Sentido – short presentation



**Sentido** is a young highly motivated company established in 2007.

● Energetic software company

● Focused on product development and consulting services

● Access to vast knowledge and experience in a number of technologies in-house and via our partners

## Experience and technologies

● Web development

● Mobile web development

● Bulgarian eGovernment services implementation

● GIS - Geographic Information Systems

● Database optimization

● Web performance optimization

● E-Services

● Splunk> integration and implementation

## Contacts

Boris Chervenkov M +359 88 8427308

@ boris.chervenkov@sentido.bg

W <http://www.sentido.bg>

## Major projects

**Tix.bg**

Real time traffic and road information management and delivery platform.

Showcase: http://www.tix.bg and <http://www.sumc.bg/map>

**KMS**

Centralized platform for systems integration, information management and e-services delivery.

Integrates more than 10 internal and external systems, and performs real-time analysis and data exchange between these systems.

Successful implementation of 4 e-services into the infrastructure of Bulgarian eGovernment infrastructure.

Client: Sofia Urban Mobility Center <http://www.sumc.bg>

**eDMS**

Product document management system, managing day-to-day work of over 100 vehicle design engineers.

Client: B&W-Fahrzeugentwicklung GmbH, Germany

http://www.b-w-fahrzeugentwicklung.de/

**eCity – electronic municipality product**

The product is end-to-end solution for municipalities, government agencies and public-sector companies.

The solution provides:

Ready-to-deploy e-service implementation, including requests, back-office management, workflow, access rights, and results delivery.

Portal – full implementation of portal features, including but not limited to content management, news, dynamic page editing, search, portal sections, media management, etc.

Client: Veliko Tarnovo Municipality

# CITA – short presentation



CITA is established in 2008 as private consulting agency in Sofia.

CITA maintains a solid infrastructure, processes, practices and tools for delivering consulting services by attracting individual experts and companies for working in teams on various projects.

CITA helps IT professionals to become top rate consultants and focus on technologies, rather than on administrative work.

The pool of experts' skills include business analysis, mobile apps development, system administration, VoIP solutions, ERP / CRM / Document management solutions and profound expertise in vast number of software technologies

## Mission and vision

Provide high-quality IT consulting with full commitment, trustiness, liability, and security.

Build and maintain a solid platform and infrastructure for delivering and consuming of IT consulting services that bridge the business with the individual experts and consulting companies.

Become a reputable authority and preferable partner that provides processes, best practices and tools for conducting high-quality IT consulting services with warranty.Consultants Database

[**Large Database of IT Professionals**](http://www.citagency.eu/about.html)

CITA maintains a large pool of consultants and tracks their based on the customers feedback. CITA constantly extends and maintains the profiles of its consultants and tracks their work.

CITA can attract the right professional for any IT project, easy and fast.

## Areas of Expertise

CITA has expertise, know-how, processes, practices and tools for establishing, planning, managing, monitoring, implementing and maintaining IT projects and services. CITA provides expertise in:

* Business
	+ Consulting model and platform implementation
	+ Project management
* Technologies
	+ Java and Java EE
	+ Microsoft and .NET Development
	+ Databases
	+ Web Development
	+ Mobile Applications
	+ Embedded Systems
	+ System Programming
	+ Network Infrastructure and System Administration
	+ Information Security
* Legal Stuff
	+ Contracts and other legal documents
	+ Accounting

# Project overview and scope

This project is the first one to implement the Korean eGovFrame in Bulgaria and in Europe, and to provide proof-of-concept and a success story for developing modern, highly scalable solutions based on the Korean eGovFrame.

Project’s goals were to implement 3 electronic services for Sofia University:

* Students’ certificate request
* Students’ GPA reports
* Science projects application

## Student’s certificate request

This public service is available to allow for students to request regular students’ certificate documents over the Internet in a secure manner.

Student’s certificates are required for a number of external institutions in Bulgaria, including the Tax agency, the Military and many others.

Most students need to request such a certificate at least twice a year.

During some peak moments hundreds of students are waiting in line in each faculty of the University for these certificates.

That’s why it is important to implement such a solution, as it will benefit both the students and the administration of the University.

## Students’s GPA reports

At least four times a year the administration of the University needs detailed reports on the average scores for each student. As this may sound as an easy task, each case requires slightly different algorithm for calculating the average score for each student. Furthermore, each faculty has its own specifics on how to deal with special situations.

These non-standard requirements push the administration to prepare the reports almost by hand, as they have to tweak many aspects on the calculation process.

The second part of this project is to ease the burden on preparing these reports on a regular basis.

## Science projects

Every year the University with the help of the Ministry of education sponsor science projects in Sofia University. The complex process of project assessment, review, documents management, application acceptance and many other activities are done by hand each year.

The third service eases the process for both the applicants and the administration for applying with a project proposal, handling the details in the process for review, and managing the information in a secure and easy to access form.

# Project management – approach and methodologies

The software lifecycle is broken into cycles, each cycle working on a new generation of the product. The our software development process divides one development cycle in four consecutive phases:

* Inception phase
* Elaboration phase
* Construction phase
* Transition phase

## Inception phase

During the inception phase, you establish the business case for the system and delimit the project scope. To accomplish this you must identify all external entities with which the system will interact (actors) and define the nature of this interaction at a high-level. This involves identifying all use cases and describing a few significant ones. The business case includes success criteria, risk assessment, and estimate of the resources needed, and a phase plan showing dates of major milestones.

The outcome of the inception phase is:

* A vision document: a general vision of the core project's requirements, key features, and main constraints.
* A initial use-case model (10% -20%) complete).
* An initial project glossary (may optionally be partially expressed as a domain model).
* An initial business case, which includes business context, success criteria (revenue projection, market  recognition, and so on), and financial forecast.
* An initial risk assessment.
* A project plan, showing phases and iterations.
* A business model, if necessary.
* One or several prototypes.

## Elaboration phase

The purpose of the elaboration phase is to analyze the problem domain, establish a sound architectural foundation, develop the project plan, and eliminate the highest risk elements of the project. To accomplish these objectives, you must have the “mile wide and inch deep” view of the system. Architectural decisions have to be made with an understanding of the whole system: its scope, major functionality and nonfunctional requirements such as performance requirements.

The elaboration phase is the most critical of the four phases. At the end of this phase, the hard “engineering” is considered complete and the project undergoes its most important day of reckoning: the decision on whether or not to commit to the construction and transition phases. For most projects, this also corresponds to the transition from a mobile, light and nimble, low-risk operation to a high-cost, high-risk operation with substantial inertia. While the process must always accommodate changes, the elaboration phase activities ensure that the architecture, requirements and plans are stable enough, and the risks are sufficiently mitigated, so you can predictably determine the cost and schedule for the completion of the development.

In the elaboration phase, an executable architecture prototype is built in one or more iterations, depending on the scope, size, risk, and novelty of the project. This effort should at least address the critical use cases identified in the inception phase, which typically expose the major technical risks of the project. While an evolutionary prototype of a production-quality component is always the goal, this does not exclude the development of one or more exploratory, throwaway prototypes to mitigate specific risks such as design/requirements trade-offs, component feasibility study, or demonstrations to investors, customers, and end-users.

The outcome of the elaboration phase is:

* A use-case model (at least 80% complete) — all use cases and actors have been identified, and most use- case descriptions have been developed.
* Supplementary requirements capturing the non functional requirements and any requirements that are not associated with a specific use case.
* A Software Architecture Description.  An executable architectural prototype. A revised risk list and a revised business case. A development plan for the overall project, including the coarse-grained project plan, showing iterations” and evaluation criteria for each iteration.
* An updated development case specifying the process to be used.

### Construction phase

During the construction phase, all remaining components and application features are developed and integrated into the product, and all features are thoroughly tested. The construction phase is, in one sense, a manufacturing process where emphasis is placed on managing resources and controlling operations to optimize costs, schedules, and quality. In this sense, the management mindset undergoes a transition from the development of intellectual property during inception and elaboration, to the development of deployable products during construction and transition.

Many projects are large enough that parallel construction increments can be spawned. These parallel activities can significantly accelerate the availability of deployable releases; they can also increase the complexity of resource management and workflow synchronization. A robust architecture and an understandable plan are highly correlated. In other words, one of the critical qualities of the architecture is its ease of construction. This is one reason why the balanced development of the architecture and the plan is stressed during the elaboration phase. The outcome of the construction phase is a product ready to put in hands of its end-users. At minimum, it consists of:

* The software product integrated on the adequate platforms.
* The user manuals.
* A description of the current release.

## Transition phase

The purpose of the transition phase is to transition the software product to the user community. Once the product has been given to the end user, issues usually arise that require you to develop new releases, correct some problems, or finish the features that were postponed.  The transition phase is entered when a baseline is mature enough to be deployed in the end-user domain. This typically requires that some usable subset of the system has been completed to an acceptable level of quality and that user documentation is available so that the transition to the user will provide positive results for all parties.  This includes:

* “beta testing” to validate the new system against user expectations
* parallel operation with a legacy system that it is replacing
* conversion of operational databases
* training of users and maintainers
* roll-out the product to the marketing, distribution, and sales teams

The transition phase focuses on the activities required to place the software into the hands of the users. Typically, this phase includes several iterations, including beta releases, general availability releases, as well as bug-fix and enhancement releases. Considerable effort is expended in developing user-oriented documentation, training users, supporting users in their initial product use, and reacting to user feedback. At this point in the lifecycle, however, user feedback should be confined primarily to product tuning, configuring, installation, and usability issues.

The primary objectives of the transition phase include:

* Achieving user self-supportability
* Achieving stakeholder concurrence that deployment baselines are complete and consistent with  theevaluation criteria of the vision
* Achieving final product baseline as rapidly and cost effectively as practical  This phase can range from being very simple to extremely complex, depending on the type of product. For example, a new release of an existing desktop product may be very simple, whereas replacing a nation's air-traffic control system would be very complex.

## Training

User

# Conformance with Bulgaria’s e-Government

During the initiation phase, it was made very clear by the Sofia University and ITCC, that these two projects will be the first step towards bringing modern electronic services to the SU ecosystem, and all systems must be planned and designed to be easily integrated into the Bulgarian eGovernment ecosystem during subsequent enhancement.

Given these requirements, both projects had to follow the guidelines of the established rules, recommendations and best practices in planning and implementation of electronic services in Bulgaria.

One of the most important documents, which has been a great influence during planning and implementation of the projects was the ORDINANCE ON THE GENERAL REQUIREMENTS FOR INTEROPERABILITY AND INFORMATION SECURITY document - referred to as **OGRIIS** from now on. This document can be found as an additional document in this report.

The OGRIIS describes in detail the requirements for information security and systems interoperability in all systems that have to interact with other systems within the ecosystem of the eGovernment.

The Korean eGovFrame is heavily based on industry-wide standards and well tested base software components and frameworks. This allows for easy integration with other systems and conformance with the ordinance:

* standard data formats such as XML are very well supported by the chosen technologies
* standard communication protocols such as Web Services are integrated within the Korean eGovFrame.
* Users management is a standard component of eGovFrame, supporting secure storage of sensitive data out of the box
* Data access is done though solid foundation of ORM mechanisms, transaction management and data source management, which greatly reduces the possibility for data loss, SQL injection attacks and other threats.

The following overview diagram of the eGovFrame outlines the major components:



Figure e-Government standard framework services

# Technology overview

## Database – goals and design

The relational database is the one of the key components in almost every modern information system.

The eServices project takes good use of the latest version of the most advanced open source RDBMS – PostgreSQL 9.1.

The main entities, around which all other information is structured, includes:

* University-specific entities:
	+ Faculties
	+ Majors
	+ Forms of education
	+ Semesters
	+ Degrees
* User-centered entities
	+ User profile
	+ Access groups and permissions
* Process-specific entities
	+ Science projects:
		- Campaigns
		- Project submissions
		- Attached documents
		- Project members
		- Reviewers
	+ Certificates
		- Certificate request
		- Payment rules
		- Reasons for issuing a certificate
* Other entities
	+ Administrative regions
	+ Cities
	+ Municipalities

On the diagram below one can easily spot the entities described above.

The database design follows the best practices for implementing such requirements.



## Deployment environment

The project has been deployed to a server within the Sofia University Infrastructure with the following characteristics:

OS: CentOS 5

RAM :2GB

HDD: 40GB

Network: 100Mbit

The application server of choice is Tomcat 6, running on Java 1.6.

The web server is Apache HTTPD.

## User Interface and design

The user interface design of the project was split in two separate parts:

* Portal interface
* Backend interface

### Portal user interface design

The goal during the design of the portal was to blend with the official Sofia University portal, so that users will not notice the transition between the two portals.

### Backend user interface design

The UI design for the backend aims for a different goal – is targets the day-to-day activities of the administrative staff.

The design must be clear, usable and easy to understand.

## User management, authentication and access rights

Authentication within the system is done via the corporate LDAP server of Sofia University.

Every user has a local profile within the system, but the main information and authentication is done by employing tight integration with the LDAP server.

# Security and threat management

The Security Architecture defines how detective and protective security controls, audit trails, and tool kits should be planned and implemented to provide integrated security across the four primitive architecture domains (business, applications, data, and technology). It is aligned with the overall architecture model and setting general security requirements

This approach is expected to lead to the following underlying benefits:

* Consistent management of risks, while leveraging industry best practices – security, like a chain, is only as strong as its weakest link. A consistent approach within the project, based on industry best practices, will result in better overall security of the Information and Telecommunication environment.
* Reduced costs and improved flexibility through common Security solutions – ones that are sharable to reduce total costs. In addition, shared solutions also reduce barriers to solution integration and interoperability, thus improving flexibility.
* Allow decision-makers to make better and faster Security-related investment/design decisions – the resulting decisions will be strategically aligned, faster, and more consistent across departments
* Promote interoperability, integration, and ease-of-access – solution access, interoperability, and integration are all enabled by strong and consistent security mechanisms.

## Approach to security architecture

**Figure 2** below illustrates the approach used to formulate the security architecture decisions.



**Figure 2 – Security Architecture Domain Project Flow**

The project flow will be broken down into four distinct sections:

1. Business and Data Architecture domain activities provide valuable input into the development of the Security Subsystem and help to describe the user categories in relation to the Security Zones of Control, by providing details on Logical Users Groups and their Logical Locations and the Data Sharing Model.
2. Data gathering activities provide additional input that help to formulate the Security Subsystems and the development of the Architecture model. Questionnaires completed by departments, workshop sessions, existing principle and policy documentation provide valuable information and insight.
3. Validation and Refinement activities further mature the Subsystem and Architecture model through workshop sessions and quality assurance reviews.
4. Security Architecture Report Preparation and Review activities allow for appropriate feedback from all Subject Matter Experts and e-Governance stakeholders to ensure a viable Security Architecture that can directly influence the Application and Technology Architecture domains.

**Inputs**

Key activities that provide input into formulating the security architecture decisions include:

1. Business Architecture defines the Architectural Requirements, Logical User Groups & Logical Locations. These provide a base of decisions that can directly influence the development of the Security Architecture.
2. Data Architecture defines a Data Sharing Design Model that could be used to test the Security Architecture as a form of a use case.
3. e‑Governance Principles and Security Policy provide principles and security policy requirements that help guide security architecture decisions.
4. Security Architecture Workshop sessions serve as a way to gather information and validate security architecture decisions.
5. Security Architecture Questionnaire provides department responses on current practices and future requirements (Authentication, Identification, User Management, Authorization, Access Control)
6. Risk Assessment activities provide a list of high-level threats and their relative impact and likelihood of occurrence to validate security architecture decisions.

## Security strategies

The following strategies are the basis of many of the architectural decisions, and can also be used to guide the security design of the project. These strategies have been extracted from generally accepted security best practices. The general security strategies are:

* + **Least Privilege** – is the concept that limits access to only what is needed to perform approved functions. An Object should have only the privileges it requires to carry out its task. Objects include individuals, applications, and other entities that can access assets.
	+ **Defense in Depth** – is the concept of relying on more than just one component or mechanism to be secure, as its failure may compromise the entire security.
	+ **Choke Point** – forces attackers to use a narrow channel of access where actions can be monitored and controlled. Commonly applied to the entrance and exit of Demilitarized (DMZ) zones
	+ **Weakest Link** – security is only as strong as the weakest link. Smart attackers will seek the weakest point to attack. It is important to be aware of the weak points in order to eliminate them or monitor them more closely.
	+ **Fail-Safe Stance** – systems should fail safely. If systems are brought down unexpectedly for any reason it is important that the system fails in such a way that it denies access to an attacker rather than grants access.
	+ **Universal Participation** – everyone needs to be concerned with security. If only one person or area opts out, an attacker may be able to mount an effective attack by first attacking them.
	+ **Diversity of Defence** – do not rely on only one (type of) system or application for security, no matter how strong or comprehensive it may be (e.g. one firewall). If it were to be compromised then other components would become vulnerable.
	+ **Simplicity** – keeping the overall environment simple makes it easier to secure. The more complex the security environment, the harder it is to guarantee it is secure. If it is very complex there could be many different types of threats that could take advantage of vulnerabilities and it would also be harder to ensure all safeguards have been applied.
	+ **Compartmentalization** – we can minimize the amount of damage that can be done to an environment (or system) if we break the environment (or system) up into as many isolated units as possible. Gaining access to one isolated unit does not provide access to the whole. All data of a similar classification may not have the same vulnerabilities or access requirements by the same user population. Therefore, isolating information assets based on vulnerabilities or segmenting network sections based on different user communities provides an additional layer of defense.

**Protect against insider as well as outsider threats** – historically, insiders account for 65% of all attacks. Protections should be such that the source of the threat makes little difference between an inside or outside attack. This can be accomplished by allowing for user management disciplines, additional levels of authentication and registration to access critical information assets.