Functional Integration Test of Mass Processes with Electronic Signatures in Public Administration

Burkhard Lüpken, Frank Losemann, Thomas Engel, Christoph Meinel
Institut for Telematics,
Bahnhofstr. 30-32, D-54292 Trier, Germany
E-mail: {luepken | losemann | engel | meinel}@ti.fhg.de

Keywords- **Integration Test, Trust Third Party (TTP), Distributed System, LDAP, Directory Server**

***Abstract*- Nowadays, almost all public administration plan to establish processes with electronic signatures. For such processes, there are no standardized system models with test cases. We are developing a simplified system model with interfaces of a public administration to determine an integration test with test cases especially for mass processes. These are very time-consuming and labor intensive. After simulating these cases, we conclude that applying a functional integration test could reduce costs for establishing a trust center[1]. We are planning to apply that method in some public administration. The first step is to analyze the actual situation of mass processes in public administration. Our system model is simple and common i.e. it could be applied for the various tiers of public administration, the European, the federal, the state and the local tier. In our age of globalization and European integration it is particularly the supranational level, i.e. the European tier, that is becoming increasingly important. In order to replace the handwritten signature with an electronic signature a trust center has to be set up. The trust center administrates the certificates of authorized officers by using electronic signatures. Therefore, it is necessary to analyze the organizational structure to determine the authorized officers of the mass processes.**

I. INTRODUCTION

Software tests aim at establishing a correct, fault-tolerant and reliable system [1]. There are diverse kinds of software tests. Integration tests take place after module tests are completed and before system tests. The module tests are part of implementing the software components. Next the integration test follows. Then the system test and acceptance test could be executed. We select the mass processes as very important and labor-intensive processes. We are planning a test to check the interfaces of the mass processes for the trust center. Th kind of test is called "functional integration test" of certain interfaces [2].

Today, electronic services are used by public administration in many ways [3]. As the world markets are in a process of deregulation and globalization, public administration in the European Community will continue to act on a supranational level [4]. The complexity of diverse administrative actions will continue to increase in public administration. It is a challenge to try to simplify the proceedings of the European Community in this age of globalization and to make it more cost-efficient. A solution might be found by simplifying and rationalizing the public sector. At the moment, many countries -especially the developing countries - are planning to reorganize their authorities and administrative offices [5].

The public administration establishes processes according to the German Signature law. We will analyze only the input and the output of the interfaces to the trust center in order to test the components of the system. The interfaces of the trust center are determined by administration actions or business processes of the trust center. By using path analysis we will able to detect the coverage of test cases. For the different test cases it is important to develop a simplified model. This simplified model should be commonly applicable for the various tiers of public administration. Nowadays, the authorities of the public administration belonging to the European, the federal, the state and the local tier. There are administrative cooperations according to the administrative law and instructions. It is depend on the administrative function. Every authority with the exception of the government departments has a superior authority. The authorities are composed of elected representatives, elected officers and administration officers. The director of an authority is the chief officer. The chief officer, authorized officers or authorized representatives sign or counter-sign administrative actions with a handwritten signature according to the administrative instructions. All administrative acts might have to be reviewed regularly by authorized authorities with their officers. For example the audit court controls periodically the financial transactions of the authorities. If the electronic signatures are generated according to the German Signature law, the court admit them in evidence [6]. To preserve the legal binding of digital signatures / digital signed documents the applications have to form a secure technical infrastructure. The trust center validates electronic signatures and helps to avoid the abuse of office.

For our system model we simplify the reality. We consider only inferior authorities with a superior authority. We use that system model to illustrate the role of mass processes in public administration. In each authority there are *authorized officers* using *the signature system*. Most of the authorities are located in the intranet. Our model is focused on internal communications. But it can integrate external communication by separating external from internal addresses and mapping them in an additional step through technical and

[1] The term “trust center” is used in the sense of “trusted third party” (TTP). It denotes an organisational entity that provides all services related to digital signatures for the organisation.

organizational processes (e.g. gateways: mails from the outside world are sent to the public department address and later redirected to the responsible officer). For simplicity's sake, in our system model the administrative actions, which have to be electronically signed by the authorized officer according to the office circulars and the administrative instructions, are called "*order*". The superior authority, the authorities, the departments and the special department for the mass processes have a software *system for computing orders* with signatures. In our model the public administration has departments at different locations. Each department has superior departments or superior authorities. All these departments can belong to various administrative districts. In such a system there are many diverse administrative actions and information processes. In Fig. 1 only the different kinds of signing processes are represented in the system model of a public administration. The organizational structure of public administration needs the following signing processes:

1) Superior Authority: The authorized officer of the superior Authority sends signed emails to other authorities and departments.

2) Authorities with a *central* signature system: The authorized officer of the authority sends signed emails via a central signature system. These signed emails are sent at the order of the director of the authority or at the order of a superior authority. The superior authority could be the local government, the district administration direction or an authority which receives its orders from the local government or the district administration. The email address of the authorized officer is: {number of the authority}.{number of authorized officer}@{name of domain-WEB-address} (e.g. department 007, authorized officer 007 of the intranet with www.ti.fhg.de 007.007@ti.fhg.de).

3) Authorities with *decentral* signature systems: for each authorized officer there is a decentral signature system. The authorized officer of the authority sends signed emails by using his signature system. These signed emails are sent at an order like in 2.. It must be clarified beforehand, if the authorized officer getting the order via his signature system has to send the signed email himself or if another authorized officer of the authority is responsible for that process.

4) Authorities *with different locations and one signature system*: like 2., but the authority with different locations and one signature system has to access one signature system from different locations.

5) *Departments* like 2., 3. and 4.

6) *Authority outside the intranet*: like 2. and 3. with the addition of encrypting the signed email before sending it via Internet.

7) *Mass processes*: Mass processes use batch jobs for signed emails. The director of a department for mass processes is the authorized officer of that signing process. There are appointed officers to represent the authorized officer. The authorized officer of the authority sends signed emails using a central signature system. These signed emails are sent at the order of the director of the authority or at the

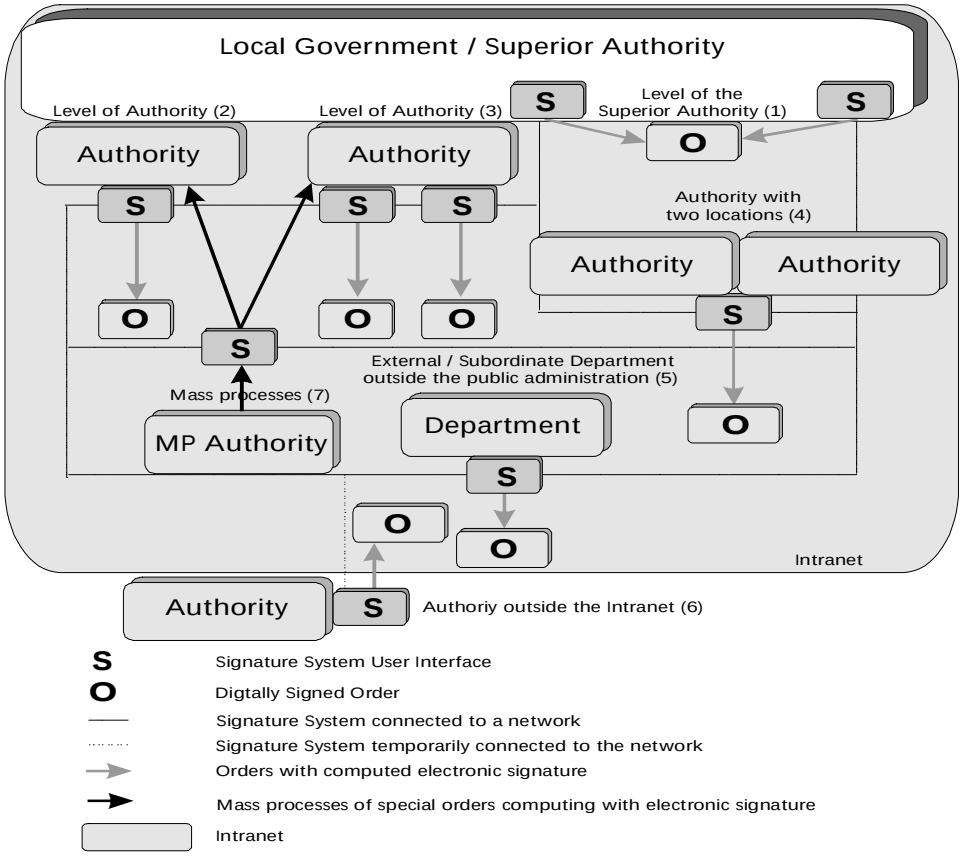

Fig. 1. Structure and Signature-Interfaces of a public administration.

order of a superior authority. The superior authority could be the local government, the district administration direction or an authority which gets its orders from the local government or the district administration. The email address of the authorized officer is: {number of the authority}.{number of authorized officer}@{name of domain-WEB-address} (for example department 007, authorized officer 007 of the intranet with www.ti.fhg.de 007.007@ti.fhg.de).

Mass processes as considered here are periodically administrative acts like e.g. paying

- Personal costs,
- Rent of official residences,
- Travelling expenses,
- Loans,
- Allowance,
- Diverse funds.

We must difference between orders which have to be signed and orders which have to counter-signed. The Trusted Third Party (TTP) has to be implemented for the authorized officer computing digital signatures and another officer or for the office authorized officer receiving the signed emails interfaces to the trust center. These interface business processes are:

1. Issuing Certificate
2. Revoking Certificate
3. Checking Certificate
4. Computing Signature

These four „business processes“ have to be integrated in the complex organization of public administration.

II. Test scenery Mass Processes

The Mass Processes have an interface to the trust center like the other interface processes in our system model. In the authority, where the mass processes are executed, we have one authorized officer, who uses the signature system to send signed orders automatically. This officer could be the chief officer. There are also some appointed officers to represent the chief officer. These officers have to be appointed. All these authorized officers need a certificate of the trust center. So we have to provide a way of obtaining / issuing personal certificates identifying the holder as member of the organization. A certificate has to be revoked, if it is not valid anymore, if the authorized officer requests the revocation, or if the operation of the trust center is terminated.

Mass processes are regularly processes with automatically signed orders (Fig. 2). That process simplifies the old process printing all orders on paper and signing them manually. We call this department or authority Mass processes (MP). In our simulation we use a server with batch process sending hundred emails per job. For receiving these signed orders we use two servers, because the orders of the mass processes could be sent to many other departments. A part of signed orders has to be countersigned. Thus, that orders has to be sign by a second authorized officer. The servers, which receives the Mass-Orders, check the certificate and the signature automatically. Existing applications for mass

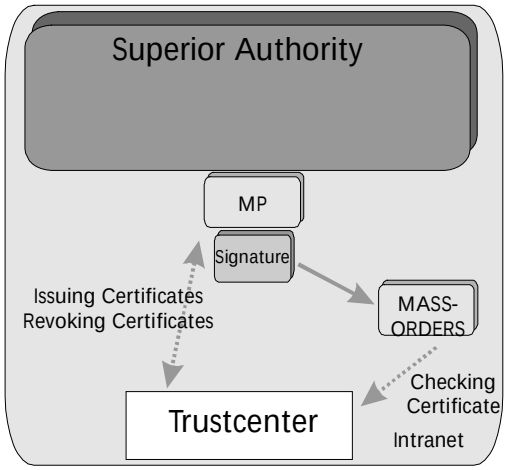

Fig. 2: Mass Processes

processes can be integrated into our model by introducing a wrapper program to encapsulate the communications of the process. The job of starting the mass process is transferred to the wrapper which can handle signed input data, check and verify the signatures and authorizations, and remove those extra data from the input stream sent to the original mass process application. The output of the original mass process application can be post-processed including an optional step of digitally signing the data.

III. Test

A Software test should consist of a test plan and test report. Our quality assurance requires the following documents [7].

A. Test Plan

We used the template of Frühauf, Ludewig and Sandmayr for a test plan [8]. The test plan consists of

1. Introduction
   - 1.1. Purpose of the Integration Test
   - 1.2. Contents of the Trust Center Integration Test
2. Test Environment
   - 2.1. Software and Hardware
   - 2.2. Time Table of the Tester
3. Criteria of Acceptance
   - 3.1. Criteria for Success or Termination
   - 3.2. Criteria for Interruption
4. Integration Test Mass Processes
   - 4.1. Introduction
   - 4.2. Tested Interface Processes
   - 4.3. Preparation of the Test
   - 4.4. Test sequence Issuing Certificates
   - 4.5. Test sequence Revoking Certificates
   - 4.6. Test sequence Checking Certificates
   - 4.7. Test sequence Sending Signed Order
   - 4.8. Test sequence Sending Countersigned Order

The first three chapters essential. These chapters describe the role of this test during the whole test process. The test process consists of a module test, integration test, system test and acceptance test. Aspects, which are tested exactly, are

specified in the sub component test description. These aspects do not need to be tested in that manner again. The aim is to optimize the test process, to select subcomponents which should be tested in an integration test before testing the whole system in the system test. All these aspects have to be described in detail. The structure chosen for the model of the test object has to be motivated. It has to consist of test sections that are given in the next chapter. In these chapters all test sequences are described in detail. All test sequences consist of test cases. A test sequence includes the whole set of test cases. For each test case there is a set of input possibilities for successful or unsuccessful outcome of the test case. For every element of that set, there are states, which are expected under condition of correctness of the system.

The administration instructions of a department Mass Processes can make it necessary to have not less than two authorized officers, one for signing and the other one for countersigning. Therefore, each of these authorized officers need one certificate to become valid users of the trust center. Then it is possible to appoint officers as representative of an authority. This representative is identified by the certificate. According to the German Signature Law, it is necessary to complete a certificate request with a handwritten signature. Then the requestors has to be prove his identity. The next steps are computing a key pair (chosen at random), in the course of which the private key is stored on a smart card. Next a certificate is created. When handing out the smartcard with the private key to the user he has to be taught about how to the smart card and the security components. All these users of the trust center described above, have the right and duty to revoke their certificate if necessary. This is done by the trust center upon signed request / notification from the owner of the certificate or an authorized representative. The receivers of signed orders have to check the validity of the signature. Therefore they need access to the certificates of the senders. The certificates are made accessible through directory servers. The contents of the certificate in X.509 format determines the storage address of a certificate in a directory, which ensures uniqueness of certified identities and eases the lookup of certificate. The last two test sequences are signed or countersigned orders. According to the administrative instructions administrative acts like personal costs, loans, funds are mass processes. In that test sequences various test cases have to be defined in order to make sure that the is valid.

B. Test Report

Each test sequence should be documented in a test report. For our integration test, we designed the following template (Table 1).

For each test case, the tester compares the achieved result with the expected result. We have test cases, where the expected result is faulty, and test cases, where the expected result is not faulty. The test result cannot be accepted only if it differs from the expected test result. In this case, we have to carry out a test for analyzing and classifying the fault.

TABLE I
TEMPLATE OF A TEST REPORT

Integration test Trust center	
Test sequence no.:	
Start	
End	
Duration	
Classifying Errors	
Functional	
Important	
not important	
Acceptance (Y/N)	
Test team	
1	
2	
3	
4	
team leader	

C. Advantages of the Integration Test

The advantage of our system model is to reduce the number of test cases by using the test path coverage in a tree model of the set of test cases. Most test cases of the test sequences are connected to the certificate management. If we check all test sequences in such a manner as described in the test plan, we can be sure - with a high degree of probability - that we are conducting a successful test. The processes of certificate management are: issuing, revoking and checking certificates.

In most applications, the X.500 directory server standard is used with the Lightweight Directory Access Protocol (LDAP) [9]. Directory services are more suitable than relational databases, because their read-to-write ratio, extensibility, distribution scale, replication scale and performance are better. But how could we test the processes of certificate management? For a functional test we do not need to test the performance and scalability. If we know, though, that the public administration will have many users, it might be better to use data distribution by storing the data in different servers. With the X.500 Directory Service, subtrees of the directory tree are able to distribute on several X.500 Server [10].

For exchanging data the LDAP Data Exchange Format (LDIF) is used [9]. It is an ASCII Text format supporting Unicode Transformation Format-8 (UTF8) character code A simple entry is:

```
dn: cn=Jim Bond, ou=Department 7, dc=intra, dc=net
  objectclass: top
  objectclass: person
  objectclass: organizationalPerson
  cn: Jim Bond
  sn: Bond
  uid: jbond
  telephonenumber: +49 651 97551 007
```

The LDAP attributes use the LDAP naming model. The distinguished names (dn) are in the first line. The user name is

Jim Bond. The other information is important in order to find the subtree, except telephone number and description.

Most products of LDAP X.500 Directory Server support the client access with a browser. The default port of LDAP is 389 TCP. The standard URL (Unified Ressource Locator) of LDAP is: [11]

<ldapurl> ::= "ldap://" [<hostport>] "/" <dn> ["?" <attributes> ["?" <scope> "?" <filter>]] with
<hostport> ::= <hostname> [":" <portnumber>]
<dn> ::= a string as defined in RFC 1485
<attributes> ::= NULL | <attributelist>
<attributelist> ::= <attributetype>
| <attributetype> ["," <attributelist>]
<attributetype> ::= a string as defined in RFC 1777
<scope> ::= "base" | "one" | "sub"

The client applications, the standard internet browsers of Netscape and Microsoft and possibly self-implemented clients use this standard URL to communicate with the directory server. For some test cases it is important to analyze unexpected results of a test by checking the attributes with a LDAP client. In the future, automatic test tools will be used. The client-server interface of the directory server is one of the most important and most used business processes. If we can find most of the faults during the integration test, we reduce the costs for system and acceptance test.

IV. Conclusions

With the component-oriented integration test we are applying a test method to integrate different modules of a software project for mass processes in public administration. The turnover of the administration acts “Mass Processes” is high. Thus, the effort of the integration test for these mass processes is maintainable. It is a new idea to use a functional integration test of this kind without knowing about the program code or the structure of the different software components. The administration apparatus has a complex structure, but for every authority or public office there are superior authorities or chief officers. If the superior authority is a government, there are elected representatives instead of chief officers. So it is possible to use our system model for various types and tiers of public administration. Such mass processes can contribute to simplify and reorganize public administration. By having a sufficient functional integration test, the establishment of mass processes is more secure than to rely on the correctness of various products, which serve as security components. Our new test method included test reports of all test sequences, so that responsible office for establishing the trust center has a protocol recording the functional correctness of that components. Thus, that responsible office is ensured, if the system does not work correctly.

References

[1] DIN ISO/IEC 9126, *Information Technology - Software product evaluation - Quality characteristics and guidelines for their use*, 1991

[2] H. Balzert, *Lehrbuch der Softwaretechnik Band II*, Bochum 1998

[3] V. J. Bekkers, S. Zouridis, *Electronic service delivery in public administration: some trends and issues*, in: International Review of Administrative Sciences - The changing world of government, Vol.: 65 1999 (2)

[4] G. Vilella, *Importance and role of supranational administration: the case of European administration*, in: International Review of Administrative Sciences - The changing world of government, Vol.: 65 1999 (2)

[5] I. Hentic, G. Bernier, *Rationalization, decentralization and participation in the public sector of management of developing countries*, in: International Review of Administrative Sciences - The changing world of government, Vol.: 65 1999 (2)

[6] “Gesetz zur Regelung der Rahmenbedingungen für Informations und Kommunikationsdienste” (Informations- und Kommunikationsdienste- Gesetz) in der (BT-Drs. 13/7934 vom 11.06.1997)

[7] DIN ISO/IEC 12119, *Information Technology - Software packages - Quality requirements and testing*, 1994

[8] K. Frühauf, J. Ludewig, H. Sandmayr, *Softwareprüfung - Eine Anleitung zum Test und zur Inspektion*, Stuttgart 1995

[9] T. A. Howes, M. C. Smith, G. S. Good, *Understanding and Deployment LDAP Directory Services*, 1999

[10] D. Chadwick, *Understanding X.500 - The Directory*, http://www.salford.ac.uk/its024/X500.htm, 1996

[11] T. A. Howes; M. Smith: RFC 1959: An *LDAP URL format available at url*, ftp://ftp.isi.edu/in-notes/rfc1959.txt; 1996