Protection Profile for Secure Sensitive Information System on Mobile Devices

Imed El Fray, Tomasz Hyla, Wlodzimierz Chocianowicz

Protection Profile for secure sensitive information system on mobile devices

Imed El Fray[1], Tomasz Hyla[1], Włodzimierz Chocianowicz[1]

[1] West Pomeranian University of Technology, Szczecin
Faculty of Computer Science and Information Technology, Poland
{ielfray, thyla, wchocianowicz@zut.edu.pl}

Abstract. The mobility of the user and information is a factor that should be taken into account during the design and development of mechanisms protecting the sensitive stored, exchanged and processed information on mobile devices. This paper discusses the security profiles for the user and dispatcher subsystems protecting sensitive information on the mobile device called MobInfoSec. MobInfoSec is a system providing users with secure sensitive documents by using the specialized class SP cryptographic module, which protects directly the trusted system components through implementing ORCON access control rules. Protection Profile defines the security functional requirements for MobInfoSec system executing the encryption/decryption of documents based on addressed access policies. The article includes a general description of MobInfoSec system, including assets, assumptions, threats, policies and functional requirements necessary for the evaluation of security functions developed in accordance with requirements of the standard ISO/IEC 15408 (called the Common Criteria).

Keywords: Mobile device, Sensitive information, Originator Controlled Access Control, Secure Protection Module, Protection Profile.

1 Introduction

Today such terms as privacy, security, mobility of users and information or mobility of the information itself are important features of the information systems that must be considered during the design and development of protection mechanisms of sensitive information. The importance of the systems dedicated to the mobile platforms has grown significantly in recent years. Mobility of information requires that the level of information protection, regardless of its location, must be the same as in the case of local information. The achievement of this level of protection requires the design and implementation of systems in the manner preventing the access to information by unauthorized entity (especially if confidential or classified information is the case).

The growing number of mobile users (private or business ones) who store sensitive data on such devices requires strong access control mechanisms. These requirements can be met by using the Originator Controlled (ORCON) access control model [1]. It

Corresponding author: Imed El Fray, e-mail address: ielfray@zut.edu.pl, full postal address: West Pomeranian University of Technology in Szczecin, Faculty of Computer Science and Information Technology, ul. Zolnierska 52, 71-210 Szczecin, Poland.

is assumed in this model that each document has its owner. However, an access must be controlled by a dispatcher of the document (i.e. the entity that has the right to share the document on behalf of the owner). The owner can determine who shares a document, but the final decision is up to the document dispatcher. The user of the document (who was given the access right from the dispatcher) can't copy it or share it with other users without the consent of the dispatcher. The solution based on ORCON model will allow the achievement of two objectives:

- security of mobile information
- release of the user from the obligation to monitor any classified information contained in his/her mobile device.

A noticeable rapid increase in the number of identified vulnerabilities and attacks on mobile systems, and the lack of a system that clearly and transparently enforces the protection of sensitive information collected from various sources and stored on mobile devices, justify the need to design and develop new mechanisms to improve the security of information processed on mobile devices.

This paper presents protection profiles for the user system of information processed and stored on a mobile device, and the dispatcher system as well. It is assumed that the mobile device allowing an access to sensitive information will be a part of the proposed MobInfoSec system described in [2]. Typically, such systems must be centralized in a way enabling each entity to download the protected sensitive information properly. The access to the system can only be obtained by the entity or entities from the group who meet the conditions specified in the access policy integrally related to the downloaded sensitive information.

Due to such features, the sensitive information will be available not only within the information management system, but also on any mobile device (called an ORCON class), in contrast with existing systems.

This paper contains the description of the ORCON access control model (in Section 2) and the description of the MobInfoSec system (in Section 3). Section 4 contains the identified assets, assumptions, threats, the security policy and selected functional requirements of the above-mentioned system, all together realizing the security goals.

2 Originator Controlled Access Control

One of the biggest challenges for the protection of the sensitive information is to create such an access control system where, under the assumption that the creator of the document (or the institution acting on its behalf) has no control over the operating user system of the document, it would be possible to control the process of sharing documents distributed by the author to the others. By using the existing cryptographic mechanisms one can protect the documents in such a way, that only an authorized person has an access to them. In contrast, it is difficult to protect them against an internal attacks, when a dishonest user having access rights to the file intends to distribute these rights further without permission of the author.

The ORCON [1] access control rules, which require that the author of the document have full control over its dissemination, allow the creation of such a system

to control an access to the classified information in order to protect the document against internal attacks. However, due to the fact that modern operating systems together with the software can be freely modified by an attacker, the effective implementation of the ORCON model is a difficult task. It results from the fact that the attacker can preview the contents of memory at any time, and thus can gain unauthorized access to a document which always must be decrypted before being displayed on the mobile device screen [2,3].

In order to achieve more functionality, the hybrid ORCON model has been created. This model combines the features of MAC and DAC models/strategies. In this model it is assumed that each resource (document) has its owner. The owner may be the author of the document, but this is not necessary. The document owner has the authority to manage his/her documents, for example he/she may have to read, write or update rights. The owner may transfer these rights to other users of the system. Users are endowed with such a right, but they cannot pass it on - this applies to the same document and all copies thereof. The access to the document can only be granted after its owner approval. This rule distinguishes ORCON model from the basic models (MAC, DAC, RBAC).

ORCON model rules proved to be particularly important in the case of the sensitive information of high importance (the security of the government institutions as an example), as suggested by the authors [4,5]. The example of using the ORCON model in this context is provided in [6].

As mentioned above, the hybrid ORCON model draws its principles from models of MAC and DAC. ORCON requirements can be fulfilled only by bringing together some of the features of MAC and DAC. The idea of this was presented in [1,6] and consists of describing the ORCON model as a function of the requirements which are fulfilled by MAC and DAC models:

- the owner of the resource cannot itself to change the access rules for MAC;
- when copying a resource, the access restrictions are copied along with the access to the resource and attributed to its copies (access to a copy is identical to the original);
- the resource originator can change the access rights of other entities too.

One can notice that the first two principles are under the control of MAC (not under the control of the owner), while the third rule is consistent with DAC and is subjected to the owner control.

The main problem related to ORCON model is of an architectural and implementation nature, i.e. how to meet ORCON objectives effectively. In this model it is important to define an arbitrary and dynamic access structure. There are many approaches for the implementation of access structures (ACL, cryptographic techniques using special SP hardware modules [1], etc.).

When building the flexible access structures, special attention should be paid to the secret sharing methods [7,8], which allow to create dynamic structures [9-11]. When designing advanced algorithms, secret sharing can tend to create structures with specific topologies or structure topology defined by the resource owner.

The detailed description of ORCON access control model (including examples) was presented in [1-3,6]. Below the protection profile of the MobInfoSec system is

described. This system is evaluated for the compliance with the requirements of the Common Criteria (EAL4 level).

3 Description of MobInfoSec system

The subject of the protection profile is the system of cryptographic protection of the sensitive information on the mobile devices (MobInfoSec). The system consists of four basic subsystems:

- Dispatcher subsystem,
- User subsystem,
- Policies and assertions management subsystem,
- Cryptographic and PKI services subsystem and two auxiliary Subsystems: standard trusted subsystem and mobile device protection subsystem.

All the above mentioned subsystems are functionally combined into a single integrated system.

The following Figure 1 highlights the important software components included in MobInfoSec system.

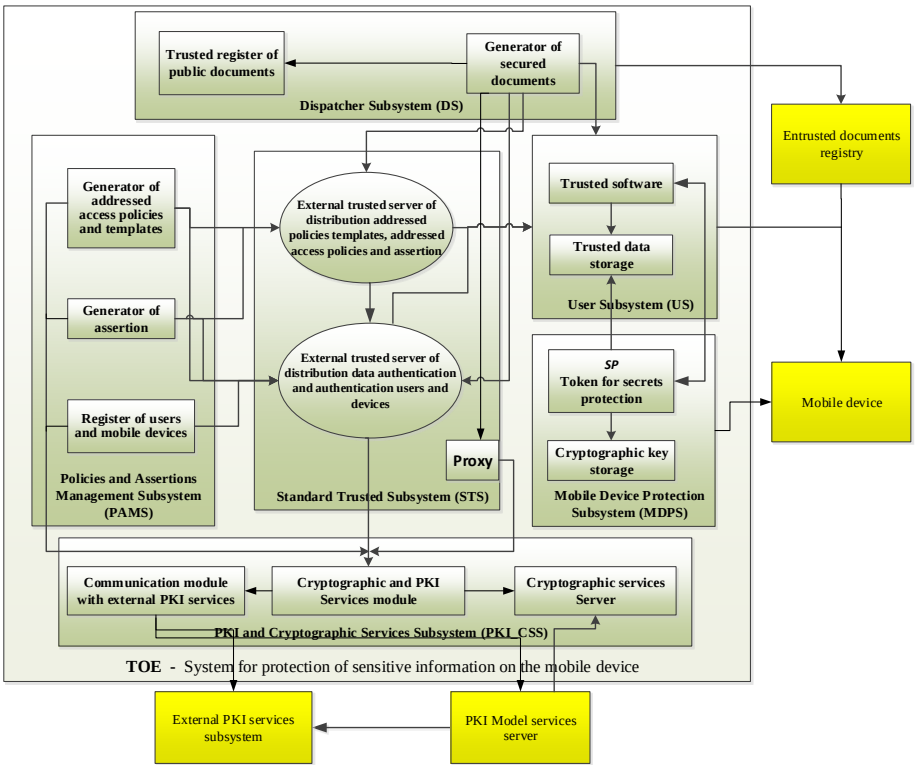

Fig.1 MobInfoSec components

3.1 Dispatcher Subsystem (DS)

DS is used to generate the addressed access policies and to encrypt documents with sensitive information in accordance with those policies. DS can be embedded on a stationary device, and on a mobile device as well. The subsystem consists of two components:

- **Trusted Register of Public Documents:** The component is responsible for collecting public documents developed by the authors, which can be encrypted by Generator of Secured Documents;.
- **Generator of Secured Documents**: The component is responsible for issuing requests to generate addressed access policies and to encrypt the specified document under the terms of the policy.

3.2 Policies and Assertions Management Subsystem (PAMS)

PAMS is used to generate and provide an addressed access policy and its templates to a standard trusted subsystem, and to generate and make available information concerning assertion users and mobile devices based on the catalogue of trusted users and devices. The subsystem consists of three following components.

- **Addressed Access Policies and Templates Generator:** The component generates the addressed access policy and its templates associated with the document in response to the request received from the DS. Generated Policies and their templates are provided and published by the trusted server, so called "Server of Addressed Access Policies and Templates". All generated policies and their templates are stored in the "Templates Magazine of Addressed Access Policies".
- **Assertion Generator:** The component allows to register, generate and publish assertions compatible with the selected profile and format, and to certify the existing imported assertions (e.g. from the server of data distribution which authenticates trusted external users and devices, confirming the different rights and privileges of sensitive information users). The generated assertions are published in the standard trusted subsystem (STS) called "Assertion Trusted Server". All generated and cancelled internal and external assertions (generated outside the MobInfoSec system) are stored in the "Assertions Magazine".
- **Users and Mobile Devices Register:** The component contains information about the users and their associated devices operating under MobInfoSec system, and their status (e.g. whether the unit is a combination of registered trusted software and SP module). Users and devices withdrawn from the registry (catalogue) do not have the right to decrypt any document containing sensitive information, regardless of their previously granted rights. Making available and removing users and devices from the system, and the relationship between them, is under the control of the "Users and Devices Trusted Server", and is registered in "Users and Mobile Devices Magazine".

3.3 PKI and Cryptographic Services Subsystem (PKI_CSS)

This subsystem is a service provider generating keys for the purpose of users and devices authentication, data encryption and decryption, and secure communication within the External PKI Services Subsystem and External PKI Services Module Subsystem. The subsystem consists of three following components.

- **Cryptographic Services Server:** The component generates and stores cryptographic keys used for authentication algorithms and data encryption/decryption (including threshold algorithms for keys sharing), assertions evidences, addressed policies templates and addressed policies.
- **Communication Module for External PKI Services:** The component implements the functionality of interface with PKI services provided by the external PKI service providers.
- **Cryptographic and PKI Services:** The component operates as a broker managing cryptographic service requests for the execution of service (e.g. service requests arising from the signing evidences from Dispatcher Subsystem, and Polices & Assertions Management Subsystem) and its results, or communicates with one of the two components described above.

3.4 User Subsystem (US)

US is used to authenticate and authorize users and mobile devices, and to distribute access policies to the mobile device. US is also used to enforce the access policy in the case of decryption. A trusted or untrusted (produced by external suppliers) application presenting the data subjected to access policy may be located in US. The subsystem consists of two main components (the Trusted Software and the Trusted Data Storage).

- **Trusted Software:** This component includes the software which integrity is protected by the main module of trusted software ("watchman") operating in MDPS (see: 3.5).
- **Trusted Data Storage:** This component is "the protected data storage" containing evidences concerning the user of the mobile device (certificates, optionally private keys and basic assertions), Root CAs certificates (trust points) and the decrypted document. The integrity of this storage is protected by the trusted software module ("watchman") operating in MDPS (see: 3.5).

3.5 Mobile Device Protection Subsystem (MDPS)

MDPS contains a dedicated cryptographic module called SP module. SP module protects directly the trusted US components implementing ORCON rules. This protection is possible by controlling the integrity of the code and configuration data. The subsystem consists of two following components.

- **Secret Protection Token:** This component provides the functionality of Trusted Platform Module (two keys, one for an authentication and one for an access to the storage), the encryption and decryption keys from Cryptographic Keys Storage,

and it includes registers and codes needed to verify the integrity and enforcing certain behaviour in the case of incorrect integrity verification (blocking the action of a trusted code).
- **Cryptographic Key Storage:** This component is used to securely store keys used to authenticate users or devices, and to carry out the operations of encryption and decryption of data.

3.6 Standard Trusted Subsystem (STS)

STS is the subsystem intermediary between DS, US and PAMS. This subsystem is used to share and distribute the addressed access policies templates and assertions, data authentication of users and devices, and serves as the register of published addressed policies. STS also works with PKI_CSS under the control of e.g. PKI Proxy Gateway. The subsystem consists of two following components.

- **External Trusted Server of Addressed Policies Templates, Addressed Access Policies and Assertions Distribution:** This component retrieves addressed policies templates of PAMS. These templates are then made available for the preparation of PD addressed access policies. Prepared addressed access policies are taken by mobile devices. This component also provides assertions to mobile devices and PD in order to implement the process of authentication and encryption/decryption of data.
- **External Trusted Server of Authentication Data Distribution and Users/ Devices Authentication:** This component distributes information about the users and devices (such as information about their groups, roles) stored in the MobInfoSec system to other components of the system, and authenticates them on request.

The detailed description of all mentioned above components and architecture of individual subsystems, together with examples of business scenarios, are described in [2]. Below, in accordance with the guidelines of the Common Criteria [12-14], the following items are defined: assets, assumptions, threats and security policy, and then the policy goals counteracting security threats and supporting the security policy and security functional requirements. The security objectives rationale for threats, security policies, etc., were deliberately omitted, because they are an effect of the aggregation of data resulting from the specified chain of events describing the threat, politics, etc., contained in the following tables.

4 Protection Profile for MobInfoSec systems

4.1 The assets off the system

This section describes the most important assets that should be protected by the system.

Table 1 The most important identified assets of the MobInfoSec system

A. Document	Electronic Document(s) for encryption/decryption. Data contained in this document must be protected against the loss of integrity and confidentiality.
A. Encrypted data	Includes encrypted document and document attributes. Data (ciphertext) must be protected against the loss of confidentiality and integrity.
A. Encrypted attributes	Data contained in addressed access policies and allowing to correct encrypt and decrypt the encrypted data. These attributes must be protected against the loss of integrity.
A. Addressed access policies	Defines the rules that should be used to encrypt and decrypt the data. Addressed access policy is managed by the system administrator and must be protected against the loss of integrity
A. Programming components of the system	Software includes executable code that implements sharing services and verification rules based on addressed access policies. This software must be protected against loss of integrity
A. Users and dispatcher data for authentication and authorization	Data allowing the user and the dispatcher to authenticate and authorize. The successful end of the authentication carries out the mobile device on standby to execute commands of an authenticated entity. These data must be protected against the loss of integrity and confidentiality
A. Validation Data	All data necessary to carry out the verification of the rights of the entity to decrypt the document. These data must be obtained from a Standard Trusted Subsystem and stored on the mobile device on which the verification is made. These data must be protected against the loss of integrity.
A. Cryptographic keys stored in the system	Cryptographic keys used by the system in order to enforce their security functions. Cryptographic keys can be present in SP module and Cryptographic Key Storage, and can be exchanged between them via a trusted channel only. These data must be protected against the loss of confidentiality
A. Audit Records	Records include the events that are audited. These events should be detected and recorded by the system. These data must be protected against the loss of availability

4.2 The assumption of the system

This section describes the assumptions concerning MobInfoSec system security environment.

Table 2. The main assumption of MobInfoSec system

AE. Configuration of MobInfoSec system	It is assumed that: – MobInfoSec is properly installed and configured (virus protection is ensured, dedicated access to the system functions, etc.); – all SF are properly configured in such a way as to ensure that the security policies will be enforced on all connections associated with the components of MobInfoSec.
AE. Access policies for sensitive information	It is assumed that an access to classified information is protected in MobInfoSec in accordance with the following principles of ORCON model: – the resource (document, classified information) has a creator who is authorized to process the document (he/she does not have permission to access rights management); – the dispatcher of resource (document, classified information) manages the access rights on behalf of the creator; – copies of the resource (document, classified information) have the same access restrictions as the original resource (nobody can create copies with other privileges); – the entity that granted the right to access the resource from the dispatcher may temporarily delegate the right to access to a third party, provided that confidence in the assertion and attribute certificates of that party will be at least at the same level as confidence in the assertion and attribute

	certificates of party delegating their rights of access.
AE. Authenticity of a policy origin	It is assumed that the addressed access policies used by TOE and their templates are authentic.
AE. Cryptographic module of a mobile device	It is assumed that the mobile device has a SP class security module. SP module directly or indirectly allows, among others: – secure storage of cryptographic objects (including keys) and data; – device authentication; – authentication and integrity check of local software enabling access to classified information; – authorize access to the document on the basis of policies, certificates and attribute assertions; – document decryption; – protection (or separation) of the portion of operational memory in which the decrypted document is stored (to protect against unauthorized reading).

4.3 The threats in the system

Threats must be identified in order to accurately determine the security requirements. Because the threat is a result of the attack on the assets, it is important to correctly identify these attacks, especially those which use the currently known vulnerabilities in mobile devices [15-16]. Table 2 shows the identified threats of MobInfoSec system.

Table 3. The most important identified threats of the MobInfoSec system.

T. Damage to the system	Accidental or intentional damage to the system. – Accidental damage to the functions and/or parameters of the system can occur, for example, when entity encrypting or decrypting data removes one or more components of hardware and/or software, which are part of the system. – Deliberate damage may occur as a result of attempts to modify the components of the system by an attacker, for example, by installing false programs or applications without the knowledge of users. This damage can lead to the creation of the invalid ciphertext, the creation of the ciphertext without the knowledge of the dispatcher of the document, the creation of the ciphertext using spoofed addressed access policies, the input data validation damage or the damage to the decrypted data, etc.
T. Unauthorized access to the system	Malicious user, process or an external entity may mask as an authorized entity to gain unauthorized access to data or system resources or misrepresent yourself as a system to obtain data authentication and authorization belonging to the entities having the rights to the encryption /decryption.
T. Modification of documents set	An attacker can modify the list of selected documents for encryption, e.g. by installing false software, applications, or as a result of damage to the system code.
T. Substituting data	One or several components responsible for the form of representation of the encrypted or decrypted data can be substituted (e.g. false application) during the process of creating the ciphertext or during the transfer of it to the mobile device in order to decrypt by the user. This threat could lead to the creation of the ciphertext based on data different from those that have been selected by the dispatcher. The same applies to the decryption process by the user.

T. Malicious or flawed applications	Applications run on a mobile device may contain malicious executable code. This code can be used unconsciously or deliberately by the author (e.g. programmer), may also be a part of the software library. Malicious applications may try to publish data to which they obtained unauthorized access. They can also perform the attacks on the system platform that will provide them with additional privileges. Malicious applications may be able to control mechanisms to capture the signals from the sensors embedded in devices (e.g. GPS, camera, microphone) and to collect in this way information and data transmitted or residing on the device.
T. Unauthorized application update	A malicious third party may attempt to deliver end-user application updates that may compromise the security functions of the system.
T. Access to communication channels	Attacker can gain access to data protected by cryptographic mechanisms during the transmission by using a trusted channel between the components of the system, modifying the data during their transfer in a manner undetectable by the user.
T. Disclosure of authenticated and authorized data	The authenticated and authorized data of an encrypting/decrypting entity may be disclosed. This includes interception by an attacker of data entered into the system, the use of any unattended mobile device without the use of adequate security during the operation decryption, performing incorrect operations misleading to the encryption/decryption entity, the attack using the full search method the value of authentication and authorizing or divining or as a result of unintentionally sent data to a destination other than that indicated by the original sender.
T. Modification of a set of addressed access policies	Malicious user can access in a manner allowing to add or remove one or more addressed access policies supported by the system. In the case of addition of policies the result can be correct validation of compliance with the policies invalid ciphertexts, and in the case of deletion it becomes impossible to verify the decrypted ciphertexts.

4.4 The security policy of the system

This section sets out the principles of an organizational nature, applicable to the system.

Tab 4 Security Policy Supporting the MobInfoSec system

P. Data Presentation	The system must have the ability to present the entity encrypting/decrypting copy of encrypted or decrypted data and it should not be allowed to encrypt or decrypt the data if one can't present the entity or entities will not be informed. If the decrypted data are presented, the system should not be allowed to make a copy of data that is not following the rules set out in the addressed access policies.
P. Encryption/ decryption of documents	The system must allow for the encryption/decryption of single or multiple documents. The authorization granted by the encryption and/or decryption of the multiple documents must be based on the same encryption attributes that are necessary for a single document.
P. Compatibility attributes	To prevent the creation of improper ciphertexts or the loss of confidentiality of the ciphertexts, the system must check if all encryption attributes selected by ciphertexting person are compatible with the addressed access policies.
P. Interruption of encryption/decryption	The encrypting/decrypting entity must be able to interrupt the process before activation key encryption/decryption.
P. Explicit agreement from the Dispatcher and the user of a document	The system must oblige the Dispatcher/User for the implementation of a set of non-trivial operations to verify their willingness to encrypt/decrypt the document before running the proper process encryption /decryption of the document(s)
P. Compliance of Certificates:	To prevent the loss of confidential data contained in ciphertexts, the system must verify that the certificates (including certificates belonging to certification

	path), which are used during the authentication and authorization of shadows owners , are compatible with the addressed access policies.
P. Authenticity of certificate	The system should monitor the presence and validity of the certification path between the certified decryption entity and trusted point specified in the addressed access policies
P. Validity of certificate	To prevent improper ciphertexts or loss of confidentiality of the ciphertexts, the system must verify that the certificate selected by the dispatcher has been successfully applied in the period of its validity in accordance with the addressed access policies.
P. Integrity of validation data	The system should control the user data integrity validation on mobile devices.
P. Management	The system must allow the operator to manage addressed access policies, certificates and assertions (adding and removing them).

4.5 Security Objectives for the system

This section defines the security objectives that correspond to the identified assumptions and threats to the system, and support its security policy.

Table 5 The main assumptions and security objectives of MobInfoSec system

O. Management	The system must allow the dispatcher to define addressed access policies and their publication, and allow the operator to manage this addressed access policies, certificates and assertions (adding and removing them).
O. Secure communication	The system provides the opportunity to build a trusted communication channel between its components and to detect any violation.
O. Data protected in communication channel	System protects the encrypted data, authenticated encryption attributes, etc., against disclosure and modification when they are transmitted between its components.
O. Update and verification of mobile device software	System ensures that any updates to the user subsystem components and SP token must be automatically verified for their invariability and their origin.
O. Monitoring system and user application	System/user application provides the ability to generate event records for the audit and to send them on request to the administrator, operator and user.
O. Removal of resident information	System ensures that all data are permanently deleted and are not available.
O. Lock of the session	The system provides mechanisms that allow the temporary suspension of unattended user session, which can be captured and allow it to resume only after re-authentication.
O. End of the session	The system should impose a limit on the time that has elapsed between the taking by the dispatcher decision to start the encryption process and the time for calculating the value of the ciphertext. The same requirements apply to the process of decrypting the ciphertext by the user. In case of detecting the state of the system lock, the session ends.
O. Authentication and authorization of the administrator, operator, etc. of the system	The system should provide the administrator, operator and user to enter their authentication and authorization data before accessing its functions and before carrying out any specific measures provided therein.
O. Integrity of services	Before the system will allow users to access the provided services, it should check their integrity and the integrity of the parameters necessary for their proper operation.
O. User's warning	The system should alert the operator encryption/decryption and allow to interrupt the process of encryption/decryption in a situation where it is impossible to present the dispatcher and the user encrypted data or the encryption attributes indicated by the identifier addressed access policies, and/or where the data encrypted or decrypted are not conform to the syntax format describing it.

O. Integrity of encrypted data	It must ensure the integrity of encrypted data formats used from the time they were formatted for the creation of the ciphertext.
O. Consent of the dispatcher/user	The system should provide the dispatcher/user mechanism enabling (on a voluntary and explicit basis) the consent to initiate the process of selecting a document or documents in order to create/decrypt the ciphertext. In addition, the system should require the dispatcher/user a non-trivial initiation of the process excluding any randomness of this decision.
O. Process interruption	The system should provide the ciphering /deciphering with the mechanism that allows it to interrupt the process of encryption/decryption before activating the appropriate key.
O. Processes protection	The system must provide protection against arbitrary interference by untrusted processes, peripheral devices and communication channels, and intruders interfering with these processes, which are used during the encryption/ decryption, and during the creation of encrypted data as indicated in the creation of ciphertext request.
O. Confidentiality of data authentication and authorization:	The system must ensure the confidentiality of authentication and authorization data which belongs to the encryption/decryption entity.
O. Integrity of addressed access policies:	Before each use, the system should inspect the integrity of the addressed access policies. The system should not allow to decrypt the ciphertext if the violations of the addressed access policies integrity is detected
O. Set of documents	After acceptance by the dispatcher a permission to encrypt documents, the system must ensure that the processed set of documents actually corresponds exactly to selected one, and encryption attributes used must be identical for each document.
O. Starting the application	The system must run the application upon the user request to allow it to present the attributes of data encryption and decryption after the encryption, without revealing their content to third parties. If the system can't run this application, it should warn the user
O. Compliance of attributes	The system should verify compliance of used encryption attributes with the addressed access policies.
O. Compliance of validation data	The system shall verify that the validation data supplied for the purpose of decrypting the data comply with the criteria of addressed access policies.
O. Time stamping	The system should provide the ability to bind to the ciphertext with the reliable timestamp, which will allow (according to the addressed access policies) to confirm the creation of the ciphertext before a certain date.
O. Validity of certificate	The system must control that the certificate selected by the encryption entity is used for its intended purpose and only during the period of its validity.
O. Certification path	The system should monitor whether there is a valid certification path between the certified entity decryption and certificate of one of the selected points of trust, as defined in the addressed access policies.
O. Compliance of certificates	The system shall verify that the certificates (including certificates belonging to certification path) used during the authentication and authorization owners of shadows addressed in accordance with a given access policy.
O. Compliance of decryption key reproducibility	The system should monitor whether the process of acquiring the shadows necessary to restore the decryption key is compatible with the target site access policies.
OE. TOE configuration	TOE must be properly installed and configured so that as soon as you start passing in a safe state. TSFs implemented on mobile devices must be configured by the administrator of TOE in order to properly support the adopted TSP.
OE. Authenticity of a policy origin	Before the addressed access policy to information and their templates are approved, the operator of TOE must ensure the authenticity of their origin.
OE. Access to PKI services	ICT environment of the TOE must ensure access to: – certificates, assertions, and other necessary validation data; – information about PKI services supporting group encryption/ decryption schemes and protocols for authentication and protection of exchanged messages; – other PKI services necessary for the proper operation of the TOE (e.g. to

	support the secure establishment of distribution channels and revocation of certificates).

4.6 The security functional requirements

To determine the security functional requirements for MobInfoSec system justifying the selection of security objectives and the relationship between these components, the requirements based on the CC [13,14] and the trust model described in [17,18] are used. The results of the selection of these security functional requirements are presented in Table 6.

Table 6. Functional requirements meeting the objectives of MobInfoSec system security

Security audit (FAU)	Audit data generation (FAU_GEN.1), User identity association (FAU_GEN.2, Audit review (FAU_SAR.1), Restricted audit review (FAU_SAR.2), Selective audit (FAU_SEL.1), Protected audit trail storage (FAU_STG.1), Action in case of possible audit data loss (FAU_STG.3), Prevention of audit data loss (FAU_STG.4),.
Cryptographic support (FCS)	Cryptographic key generation (FCS_CKM.1), Cryptographic key distribution (FCS_CKM.2), Cryptographic operation (FCS_COP.1),.
User data protection (FDP)	Export of user data with security attributes (FDP_ETC.2), Subset information flow control (FDP_IFC.1), Simple security attributes (FDP_IFF.1), Import of user data with security attributes (FDP_ITC.2), Full residual information protection (FDP_RIP.2), Advanced rollback (FDP_ROL.2), Stored data integrity monitoring and action (FDP_SDI.2),
Identification and authentication (FIA)	SSF Generation of secrets (FIA_SOS.2), Timing of authentication (FIA_UAU.1), User authentication before any action (FIA_UAU.2), Protected authentication feedback (FIA_UAU.7), Timing of identification (FIA_UID.1), User identification before any action (FIA_UID.2),
Security management (FMT)	Management of security functions behaviour (FMT_MOF.1), Management of security attributes (FMT_MSA.1), Static attribute initialisation (FMT_MSA.3), Management of SSF data (FMT_MTD.1), Specification of Management Functions (FMT_SMF.1), Security roles (FMT_SMR.1),
Protection of the SSF (FPT)	Basic internal SSF data transfer protection (FPT_ITT.1), Simple trusted acknowledgement (FPT_SSP.1), Time stamps (FPT_STM.1), Inter-SSF basic SSF data consistency (FPT_TDC.1), SSF testing (FPT_TST.1),
System access (FTA)	SSF-initiated session locking (FTA_SSL.1), SSF-initiated termination (FTA_SSL.3), Default system access banners (FTA_TAB.1), System session establishment (FTA_TSE.1)
Trusted path/channels (FTP)	Inter-SSF trusted channel (FTP_ITC.1), Trusted path (FTP_TRP.1),

5 Summary

This article provides an overview of a system for cryptographic protection of sensitive data on mobile devices, implementing the functionality resulting from the requirements of ORCON model and information mobility. It presents the most important security functional requirements imposed on this type of system working in a distributed environment. The law on protection of Sensitive Information [4], the most representative ISO/IEC standards [12,14,19], all analysed attacks, especially those that use currently known vulnerabilities in mobile devices [15,16], and security profiles for mobile devices [19-21] were taken into account in order to accurately

identify the possible threats, define the security policy and security objectives to minimize the impact of threats and support the activities stated in the security policy.

Acknowledgment. This scientific research work is supported by National Centre for Research and Development (NCBiR) of Poland (grant No PBS1/B3/11/2012) in 2012-2015.

References

1. C. Yu-Yuan and R. B. Lee, "Hardware-Assisted Application-Level Access Control", In: P. Samarati et al. (Eds.): ISC 2009, LNCS 5735, 2009, pp. 363-378.
2. T. Hyla, J. Pejaś, I. El Fray, W. Maćków, W. Chocianowicz, „Sensitive Information Protection on Mobile Devices Using General Access Structures", ICONS-IARIA, 2014, pp. 192-196
3. J. Pejaś, T. Hyla, J. Kryński, „ORCON access control monitored by the initiator: theoretical and practical implementation method", National conference on Cybercrime and Information Security, Warsaw, Poland (21 pages), 2012
4. Protection of sensitive information, Polish Act of 5 August 2010, Dz.U. 2010 nr 182 position 1228
5. B. Hołyst, J. Pomykała, „Cybercrime, information security and cryptology, Prosecution and Law, Poland (30 pages), 2011
6. M. Bishop "Computer Security: Art and Science", Addison Wesley, 2002
7. A. Shamir "How to share a secret", Communication of the ACM 22 (1979), pp. 612–613.
8. G. R. Blakley, "Safeguarding cryptographic keys", AFIPS, 1979, pp. 313–317
9. J. Benaloh and J. Leichter, "Generalized secret sharing and monotone functions", in CRYPTO '88: Proceedings on Advances in cryptology, pp. 27–35, New York, NY, USA, 1990. Springer-Verlag New York, Inc.
10. T. Tassa, "Hierarchical threshold secret sharing", Journal of Cryptology, vol. 20(2007) pp. 237-264.
11. B. Nakielski, J. Pomykała, "Simple dynamic threshold decryption based on CRT and RSA", Journal of Telecommunications and Information Technology 2 (2009), pp. 70-73
12. ISO/IEC 15408 "Information technology — Security techniques — Evaluation criteria for IT security", Part 1: Introduction and general model, 2012
13. ISO/IEC 15408 "Information technology — Security techniques — Evaluation criteria for IT security", Part 2: Security functional requirements, 2012
14. ISO/IEC 15408 "Information technology — Security techniques — Evaluation criteria for IT security", Common Methodology for Information Technology Security Evaluation, 2012
15. Fortinet's FortiGuard Labs "Reveals Newest of mobile Malware Trends in Latest Threat Report", http://www.fortinet.com/ resource_center/whitepapers/threat-landscape-report-2014.html
16. F-Secure "Mobile threat report" http://www.f-secure.com/static/doc/labs_global /Research/ Mobile_Threat_Report_Q3_2013.pdf
17. I. E Fray," Method of determining the trust in the information system based on the process of assessing and treating risk", monograph Informatics, West Pomeranian University of Technology of Szczecin, 2013
18. I. E Fray, "About some application of risk analysis and evaluation", Kluwer International Series in Engineering and Computer Science, Vol. 752 (2003), pp. 283-292
19. Protection Profile for Mobile Device Fundamentals, NIAP, 2013,
20. Protection Profile for Mobile Device Management, NIAP, 2013
21. Protection Profile for Network Devices, NIAP,2012