

Russia's SORM project

(June 15, 1999) Below are two drafts of Russia's SORM project. SORM is designed to give Russia's Federal Security Bureau (FSB, the successor to the infamous KGB) the ability to view all Internet users network transactions in real time. The FSB would be capable of viewing every Russian Internet user's activity on the Web, including credit card transactions, e-mail messages, and visited Web pages.

SORM is currently under review by Russian courts on charges made by a Russian human rights organization that it is in violation of the law.

----- Approved -----

Deputy Director Federal Security Service A.A. Bespalov

" ____ " _____ 1998 Confirmed " ____ " _____ 1998

TECHNICAL REQUIREMENTS TO THE SYSTEM OF TECHNICAL MEANS PROVIDING FOR THE FULFILLMENT OF EFFICIENT RESEARCH MEASURES IN THE DOCUMENTED TELECOMMUNICATIONS NETWORKS

Approved Head of the Telecommunications Management A.Yu.Rokotyan

" ____ " _____ 1998. First Deputy to the Director General Of the Central Research Institute of the State Telecommunications of Russia Yu.A.Alekseev " ____ " _____ 1998.

1. PURPOSE

1.1. The system of technical means destined to provide for the system of efficient research measures (SORM) in the networks of the documental telecommunications (NDTC) is being arranged at the basis of the Russian Federation legislation and is meant to provide for technical support of the above research measures in the telecommunications networks which are used for supplying customers with telematic services, data transmission services, an access to the world global information network of INTERNET

1.2 The actual technical requirements (TR) concern all NDTC regardless of their forms of ownership formed previously or being currently formed according to the Russian State Communications Committee licenses.

1.3. SORM should provide for reading of all information (both incoming and outgoing) belonging to the specific subscribers of the network(s) in question.

1.4. The actual TR should be observed regardless of what means of information protection may be used in the NDTC.

1.5. The actual TR should be observed while providing additional services to the NDTC subscribers.

1.6. The actual TR should be observed for each individual subscriber regardless of the type of his connection to the DTC networks (individual or collective).

2. SET OF EQUIPMENT

The set of SORM equipment should include: hardware and software means (HSM) providing for the requirements fulfillment by SORM, these means should be part of the distant control center (DCC) ó HSM SORM DCC; hardware and software means (HSM) providing for the requirements fulfillment by SORM these means should be part of the NDTC node equipment ó HSM SORM NDTC; communication channel (communication lines and channeling hardware) providing for establishing of communication between HSM SORM DCC and HSM SORM NDTC; Note: The channeling hardware should be part of the HSM SORM NDTC equipment. SORM software security and confidentiality protection means.

3. GENERAL REQUIREMENTS FOR THE SORM ORGANIZATION

3.1. NDTC SORM management should be controlled from the DCC by way of its cooperation with the HSM SORM DCC via communication channels providing for controlling commands transmission from the DCC to HSM SORM NDTC and for information transmission from HSM SORM NDTC to the DCC.

3.2 SORM should provide for transmission of the following information from the HSM SORM NDTC to the DCC: about the HSM SORM NDTC readiness;

about the results of DCC commands fulfillment; about unauthorized interference with the HSM SORM NDTC work.

3.3. SORM should provide for transmission to the DCC the NDT subscribers data base with the following information about subscribers at the request of the DCC operator: registration date in the DTC networks; electronic address; registration address; additional services provided (including Internet roaming (and voice communication services)).

3.4. At the DCC command SORM should provide for receiving of the following information pertaining to any individual user: statistic information reading; reading of information (both incoming and outgoing) belonging to specific subscribers. Note: This command may be documented by the communications operator.

3.5. SORM should provide for determination of: subscriber's telephone number if he uses common carrier telephone line (providing this line allows for this) for using telematic services and data transmission; subscriber's electronic address if the latter uses other telecommunication networks for using telematic services and data transmission.

3.6. While reading statistical information SORM should provide for transmission of the following information to the DCC HSM SORM NDTC: period of work in the NDTC; telephone or commuted telephone line number or network address (of an other network) used for NDTC access; network addresses used for reception or transmission of information via NDTC.

3.7. While reading information SORM should provide for transmission of the following information to the DCC HSM SORM NDTC: period of work in the NDTC; telephone or commuted telephone line number or network address (other network address) used for NDTC access; real-time information transmitted via NDTC and belonging to specific subscribers.

3.8. The SORM reaction time from the moment of DCC command transmission to the moment of its fulfillment confirmation by the HSM SORM NDTC reception should not exceed 30 seconds (excluding the communication services access discontinuation).

4. HSM SORM NDTC AND HSM SORM DCC COMMUNICATION INTERFACE

4.1. Communication between SORM and DCC should be conducted via the data transmission channel.

4.2. Data transmission channel reservation should be provided.

4.3. Switch to the reserve channel should be provided in case of the main channel fault.

4.4. The information exchange should be conducted via isolated communication channel in a duplex regime at a speed not less than maximally allowed for the NDTC subscribers.

4.5. Interface of communication with the channeling equipment should comply with the ITTU recommendations V.36, V.24, G.703.

4.6. Protocol of digital data exchange between SORM and DCC should comply with the X.25 ITTU recommendation (edition of 1995) for single chain LAPB procedure.

Note: When protocols used for the networks information exchange differ from those recommended by the ITTU X.25 (such as TCP/IP), the protocol of information exchange between SORM and DCC may differ from the protocol mentioned in paragraph 4.6. as agreed with the FSB of Russia and the network administration.

4.7. The protocol of connection between SORM and DCC (the type of service information, SORM/DCC interaction algorithm, arrangement of the information transmission) should be defined in the process of SORM software development by agreement with the FSB of Russia.

5. SORM EFFICIENCY CONTROL

5.1. Functional control of the SORM hardware and software efficiency against the background of the NDTC equipment functioning should be provided for during the exploitation.

5.2. DCC should receive information concerning faults interfering with the work of the NDTC SORM.

5.3. Performance control of the information exchange channels between SORM and DCC should be provided for. In case of the damage of information exchange equipment data transmission should be canceled and a corresponding message should be transmitted to the maintenance personnel while automatic switch on to the reserve channel should be fulfilled.

6. UNAUTHORIZED INFORMATION ACCESS CONTROL

6.1. The possibility of unauthorized interference with the process of functioning and interaction between the HSM SORM NDTC and HSM SORM DCC should be excluded.

6.2. The possibility of unauthorized access to the data and software providing for the HSM SORM NDTC interaction should be excluded.

6.4. DCC should receive reports on all attempts of unauthorized access and interference with the HSM SORM NDTC functioning.

6.5. Information exchange between SORM and DCC should be secured.

7. SORM INITIALIZING AND RESTART

7.2. In case of SORM node software restart the information about this fact should be transmitted to the DCC.

7.3. Technological conditions of the SORM node software restart should include the procedure of HSM SORM NDTC restart.

7.4. A possibility of restarting part of the software controlling the work of the HSM SORM NDTC should be provided for at the DCC command.

Approved Deputy Director of the Federal Security Service of the Russian Federation
A.A.Bespalov

" ____ " _____ 1998 Confirmed " ____ " _____ 1998

THE ORDER OF IMPLEMENTATION OF THE SYSTEM OF THE EFFICIENT RESEARCH MEASURES IN THE DOCUMENT TELECOMMUNICATIONS NETWORKS

First Deputy to the Director General of the Central Research Institute of the State
Telecommunications of Russia

Yu.A.Alekseev

" _____ " _____ 1998

Administrations of the telecommunications documental networks (DTC) including the services of data transmission, telematic services, Internet informational resources access services that are guided by the «Technical Requirements To The System Of Technical Means Providing For The Fulfillment Of Efficient Research Measures In The Documental Telecommunications» should conduct the following technical and administrative operations. A plan of measures to be taken in order to implement the system of efficient research measures (SORM) in the network consisting of two stages (the first stage may be missing) should be developed and coordinated with the Federal Security Service of the Russian Federation. The first stage ó implementation of limited functions SORM using standard equipment of the telecommunications provider, experimental running of the system and evaluation of its compliance with the main technical SORM requirements. The second stage ó full fledged SORM implementation considering the results of the experimental exploitation.

The first stage provides for:

1. Development and coordination with the FSB of the technological scheme and SORM functioning algorithms at the telecommunications operator's network based on the technical requirements.
2. Correction if necessary of SORM technical requirements considering the results of the first stage implementation.
3. Development of the list of SORM hardware and software used at the first stage and according to the results of the first stage (stating type, cost, supply conditions and payer for each item).
4. Preparation of proposals and coordination with the FSB of Russia of the necessary communication protocols for data exchange between SORM equipment and standard equipment of the telecommunications provider if the provider complies with the SORM technical requirements (stage 2).
5. Purchase and delivery of the SORM equipment in accordance with the list provided above.
6. Allocation of necessary technical means for checking and tuning of the SORM software at the provider's equipment.

8. Organization of the intercity communication line between telecommunications operator and the DCC.
9. Preparation of the exploitation and technical documentation for the SORM including the regulations for the duty services interaction.
10. Testing and tuning of the SORM hardware and software during interaction with the telecommunications operator standard equipment.

The first stage is completed as the SORM acceptance report is signed and it is accepted for experimental exploitation as the result of the joint tests (FSB as the contractor and the telecommunications operator as the performer.)

The second stage provides for:

1. Development of the SORM requirements for the telecommunications operator equipment based on the Technical Requirements To The System Of Technical Means Providing For The Fulfillment Of Efficient Research Measures In The Documental Telecommunications (adjusted if necessary according to the results of the first stage) containing the list of: hardware and software means providing for the implementation of the SORM requirements and included into the equipment of the node (nodes) of DTC network ó HSM SORM NDTC; hardware and software means providing for implementation of the SORM requirements and included into the DCC equipment ó HSM SORM DCC; type of channel for communication between NDTC and HSM SORM DCC; type of equipment for the communication channel between the HSM SORM NDTC and HSM SORM DCC; the data exchange velocity between the HSM SORM NDTC and HSM SORM DCC; protocol of the data exchange in the communication channel between HSM SORM NDTC and HSM SORM DCC; protocol of junction between HSM SORM NDTC and HSM SORM DCC; information security and privacy protection software for the SORM. Telecommunications operator should coordinate technical requirements with the FSB of Russia.
2. The specification of the specific hardware and software that should be included as part of the standard equipment of the telecommunications operator and of the DCC (stating type, cost, supply conditions and payer for each item) is compiled according to the technical requirements. The specification is coordinated by the telecommunications operator with the FSB of Russia organs.

3. Technical design development for the SORM implementation by the telecommunications operator's enterprise is fulfilled by the organization licensed for the fulfillment of design works by the order of the telecommunications operator.
4. Development of the SORM technical exploitation documentation including regulation for duty services interaction.
5. SORM equipment assembling at the telecommunications operator's enterprise is fulfilled by the organization licensed for the fulfillment of assembling works by the order of the telecommunications operator.
6. Testing and tuning of the SORM software at the telecommunications operator's equipment.
7. Conducting joint SORM tests (FSB of the Russian Federation as a contractor and the telecommunications operator as a performer). The second stage is concluded with the SORM industrial exploitation acceptance report which is jointly approved by the telecommunications operator management and the FSB of Russia representatives.