EUROPEAN COMMISSION
DIRECTORATE-GENERAL
HUMAN RESOURCES AND SECURITY
Directorate HR.DS - Security
Informatics Security

Brussels, 06/09/2011
HR.DS5/GV/ac ARES (2011) 940807
SEC 20.10.05/04 - Standards

European Commission

Information System Security Policy

C(2006) 3602

GUIDELINES ON ACCESS CONTROL AND AUTHENTICATION

Version 4, 05/09/2011

TABLE OF CONTENTS

1. INTRODUCTION

In the security standard on authentication [1], the Commission defines rules and procedures for user identification and authentication. Possible implementations of those rules and procedures are described in the following guidelines.

The guidelines begin with recommendations for the structure of UserIDs and for the implementation of a user password management process. Next, detailed recommendations for possible types of authentication in information systems are described. General recommendations for the selection of user passwords are also included.

The most important part of the guidelines is the recommendation of different authentication methods suitable for SPECIFIC information systems as defined in the Implementing Rules of Commission Decision C(2006)3602.

Finally, there is a suggested outline for the Access Control Policy which must exist for all systems.

2. OBJECTIVE

The objective of these guidelines is to provide additional advice on good practices for the implementation of the rules in the Standard on Access Control and Authentication.

3. IMPORTANT DEFINITIONS

See the *Standard on Access Control and Authentication* for definitions of terms used in this document.

4. IDENTIFICATION AND AUTHENTICATION MANAGEMENT

4.1. Recommendations for UserIDs

(1) Each individual user should not have more than the minimum set of UserIDs needed for performing his/her tasks.

(2) UserIDs for standard (i.e. non-privileged) access should be composed of the first 5 letters of the user's last name and of 2 letters of the first name.

(3) UserIDs for administrative (i.e. privileged) access should be composed of the prefix "ADMIN", the first 5 letters from his/her last name and of 2 letters from his/her first name.

(4) UserIDs of tokens serving for remote access to the Commission information systems may be built differently depending on the technology used – an example is to compose them of "T" letter and 7 digits corresponding to the token number.

(5) UserIDs for systems (i.e. used by one application to access another), often termed "System accounts", should be named in a way that distinguishes them from user accounts (e.g. starting with "SYS_").

4.2. Recommendations for requester identity verification

(6) For proof of identity, the requester should provide a valid personal identification card or passport.

(7) The requester should at least once personally visit the registering office during the identity proofing process.

(8) The type and number of the photographic identification document provided, the name of the executing officer and the result of the identity proofing should be documented and stored. The staff management system may be used for the registration of the information about the requester.

4.3. Recommendations for the initial temporary password

(9) The system administrator / operator should use a password generation utility that generates random password strings and checks the uniqueness of the string.

(10) After that the user's account should be created with this generated password and with the switch for forcing the user to change the password immediately after the first logon activated.

(11) The initial password may be communicated to the user by any of a number of different ways as long as it is secure, for example:

(a) directly to the person

(b) via secure electronic mail such as SECEM (for systems other than the mail system itself)

(c) in a sealed envelope

(d) using a trusted courier

(12) The new user should be informed about the rules of good conduct to be observed for information system access and the ways in which a password can be changed.

4.4. Recommendations for "replacement" temporary passwords

(13) A Service Desk (in charge of password resets) should use a special procedure or special tools for user identity verification and new password setting (password reset) in case of users having forgotten their password.

(14) This procedure may be initiated by the user sending a request to the service desk using different channels: a unique time-limited HTML page, paper-based request sent physically or by an email from the user's unit.

(15) In case the user request is made by phone, the calling user may be identified by one or more of the following methods:

(a) using a shared secret that is only known by the service desk and the user and that is different from the forgotten password or personal identification number;

(b) using another system to which the user has authorised access, such as sending an email through SECEM with information or a one-time pass code that the user can quote;

(c) by a phone call back to a previously registered phone number (e.g. to the user's mobile phone if he or she called from a different phone).

(16) Password resets for privileged users should be subject to stronger checks. Where possible, this should include the physical presentation of the privileged user with his or her identification document (if the user is not personally known to the person performing the reset).

(17) Password resets for system accounts should be requested by the person who is responsible for the account, following the appropriate procedure depending on the level of rights granted to the account.

5. INFORMATION SYSTEM ACCESS IDENTIFICATION AND AUTHENTICATION

5.1. Recommendations for user identification and authentication

(18) The access password for a generic/default accounts (root, Administrator, DBA etc.) may only be granted to one person at a time, as specified in the Standard on Access Control and Authentication. However, a procedure may be implemented to allow the use of such accounts in emergency situations

when the account owner is absent (e.g. a sealed envelope in a safe with an approval process and a usage log).

5.2. Certificate- and token-based authentication

(19) Tokens are considered to be secure and tamper-proof devices. The following types of device – smart phone, Personal Digital Assistant – may not be considered as tokens; in fact, they are more like standard personal computing systems.

6. USER AUTHENTICATION METHODS

(20) Different industry-standard methods exist for authenticating users. Generally, it is accepted that the different forms of authentication are categorised by the number of factors they incorporate for the verification. The three factors usually considered in the authentication process are:

(a) What a user knows (a secret), such as a password, a Personal Identification Number (PIN), or item of personal information.

(b) What a user possesses, such as a token: examples of tokens might include swipe cards, smart cards, mechanical and electronic keys.

(c) What a user is (a biometric), such as a fingerprint, a retina pattern, or a voice pattern or behaviour pattern.

(21) While a simple password or a PIN may be adequate authentication for less sensitive information (PUBLIC or LIMITED BASIC), a more secure method or even a combination of at least two methods (two factor authentication) is necessary to ensure appropriate access to more sensitive or critical information or systems (above LIMITED BASIC).

6.1. Recognised user authentication methods

(22) The following eight methods of authentication are recognised by the Commission for accessing information systems, applications and data (ordered from lowest to highest security/confidence level).

M1 — No authentication. Access without authentication is suitable for applications, information systems or other IT services that provide read-only access to data classified as "PUBLIC" and for which wide internal or external dissemination is desirable.

M2 — Personal Identification Number (PIN). PIN authentication is suitable for selected "special-purpose" inquiry/update transactions or services (for example self-service processes - those that provide individuals with access only to their own records and information) or for token protection. PIN authentication may be appropriate for applications such as user registration or individual user access to their individual application specific records and information that is not considered sensitive. If desired, the PIN validation dialogue can be transmitted via a secure communications channel.

M3 — Password or pass-phrase. Password authentication should be used where the access to data or information systems requires individual (personal) and unique identification and where a medium level of individual accountability is needed. Pass-phrases are much longer (typically 20 to 40 characters) than passwords and may contain spaces; their length makes them more secure against dictionary attacks than standard passwords.

M4 — Certificates with software storage of private key. This authentication method gives a high level of individual accountability and allows better implementation of confidentiality measures on the authentication process. When it is not stored in a secure storage (e.g. password protected file, Windows registry) the private key is vulnerable to an offline brute force attack. Hence the private key storage should be protected with a password or with a higher protection method.

M5 — Token-generated password or pass-phrase. A token is an additional security protection, requiring the user to both physically possess the token and know the associated PIN. This level of protection should be used when a high level of individual accountability is needed.

M6 — Certificates with hardware storage of private key. This provides a highly secure authentication level because the user's private key is stored on a secure physical device (e.g. smartcard, secure USB token, hardware crypto board). The private key storage should be protected with a good quality password. This authentication method gives a very high level of individual accountability and allows better implementation of confidentiality measures on the authentication process.

M7 — Biometrics. This authentication method ensures a highly secure process of personal identification and verification. Biometric authentication provides a more robust and accurate authentication solution than traditional authentication mechanisms because of the uniqueness of the validation process and its convenience and ease of use. Biometrics-based authentication eliminates the problems associated with user password management. This authentication method is required when near-absolute individual accountability is needed.

M8 — Certificates with biometric protection of private key. The private key is protected with a biometric recognition system. This authentication method gives a near-absolute level of individual accountability. This is the most secure authentication level.

6.2. Authentication methods matrix

(23) The following matrix provides recommendations that the System owner may follow in terms of authentication methods for SPECIFIC information systems. It also provides recommendations for STANDARD information systems as long as the mandatory requirements described in the *Standard on Access Control and Authentication* are followed. These decisions should be approved after a risk assessment. The table considers non EU-Classified information systems with the following remarks:

– The authentication methods are referred to by from M1 to M8, which are described in section 7.

– The sign X means recommended method and the sign (X) means a reasonable method.

– Authentication methods using biometrics are not considered reasonable for non-EU-classified information.

	PUBLIC	**LIMITED BASIC**	**LIMITED HIGH**	**Remote access to LIMITED BASIC or LIMITED. HIGH**
Authentication Method				
M1	**X**			
M2	**(X)**			
M3	**(X)**	**X**		
M4		**(X)**	**X**	
M5		**(X)**	**(X)**	**X**
M6			**(X)**	**X**
M7				
M8				

7. SELECTION OF QUALITY PASSWORDS

(24) Quality passwords should have sufficient length and should be:

(a) Easy to remember.

(b) Not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers, and dates of birth etc.

(c) Not vulnerable to dictionary attacks (i.e. do not consist of words included in dictionaries).

(d) Free of consecutive identical, all-numeric or all-alphabetic characters.

(25) Recommended methods for choosing quality passwords are the following:

(a) String several words together (also known as a pass phrase).

(b) Shift a word up, down, left or right one row on the keyboard.

(c) Combine punctuation or numbers with a regular word.

(d) A mix of at least three of the following:

- Lower case characters
- Upper case characters
- Numbers
- Special characters.

(e) Create acronyms from words in a song, a poem, or another known sequence of words.

(f) Deliberately misspell a word but do not use a common misspelling.

(g) Another suitable method for choosing and day-to-day usage of quality passwords is to use printed password grids containing matrices of randomly generated characters.

8. ACCESS CONTROL POLICY

As mentioned in the *Standard on Access Control and Authentication*, each system must have an Access Control Policy which describes and governs the accesses that may be granted to the system. This section contains a suggested structure and outline of the contents of the Policy.

The Access Control Policy may contain sensitive information. If so, its distribution should be restricted on a need-to-know basis.

1. Introduction

The introduction should specify the system and its high-level functions, and state that the accesses granted within the system must be in line with the policy. It should state that the policy is approved by the System Owner.

2. Context

This section gives the context of the access policy, i.e. describing the system, the data, the functions performed by the system and the user population. All of this information is necessary to determine the appropriate access methods and rights. If this information is already documented elsewhere (e.g. in the Security Plan), then this section may simply refer to the other documentation as long as it is sufficient for the needs of the Policy.

The following subsections should be documented:

System: overview of hardware, software, network connections and physical locations in use

Data: a description of the information handled by the system, to a level of granularity that is sufficient for the definition of different accesses and roles. This section should identify and distinguish data for which this system is the master, or owning system, and which data is taken from other systems (and whether it is read-only, or modified by this system)

Functions: the functions that the system performs on the data. Distinguish read access, creation and modification of data; also any dispatch of data outside the system (e.g. to other systems or people, via automated interfaces or emails etc.).

Users: list all of the different categories of users of the system. These should first be classified as Commission Staff (including Officials, Seconded National Experts, retired staff, trainees etc.), Third Parties (e.g. contractors or MSs) or Public Users (e.g. European citizens). Next, they should be split by functions, with particular focus on any sensitive roles (system administrators, people updating sensitive data or making financial transactions etc.).

For sensitive systems, it may be useful to document any specific hostiles who would have an interest in gaining unauthorised access to the system (e.g. foreign intelligence services, terrorists, industrial spies…).

'Users' may also include other systems that access this system.

3. User ID Scheme

Describe the naming scheme that is in place for user IDs (see section 4.1 above).

4. User Authentication Scheme

Describe the authentication method(s) in use. There may be more than one method in use, e.g. for remote access or external users.

This section should also detail any quality standards in place over the authentication methods, such as password quality controls (password length, lifetime etc.).

5. Definition of Roles

Access must be role-based, and so the different roles (sometimes termed 'groups') that are created in the system must be defined and documented. Each role should be listed and described, detailing its access rights (e.g. read / create / modify / delete for specific data sets). Incompatible roles (i.e. roles which must be segregated) should be flagged, for example "Make payment" and "Approve payment".

Any possibilities for self-registration, guest or anonymous users and their permitted roles should be specified here.

Roles should include access that is granted to other assets of the system, not only information or functions, such as server hardware, software, printers, access to physical locations (e.g. data centres) etc.

6. Delegated Roles

Some systems permit users to delegate roles to other users (such as electronic mail systems allowing a team member to send an email on behalf of the team leader, or to grant approvals in his or her name). Where this is possible, the access control policy should specify which roles can be delegated and under what circumstances.

Delegated roles should be clearly identified, traceable and consultable, for both the giver and the receiver of the roles (and corresponding access rights). It should be possible to grant delegations for a specified time period (e.g. during one person's holidays).

Where delegated access rights have been used, this should be clearly flagged in the system (e.g. by showing "on behalf of" and the original user's name).

7. Access Control Processes

Describe the processes that are used to request, grant, review and revoke user accesses (including responsibilities). Specify the user identity proofing mechanisms to be used for the granting of access.

Separate processes may be required for internal users and third parties.

9. REFERENCES

Commission Decision C(2006) 3602 of 16/8/2006

Implementing Rules for Commission Decision C(2006) 3602 of 16.8.2006

Standard on Access Control and Authentication

Standard on Asset Management

Standard on Risk Management

ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management

NIST SP 800-63-1 Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology, December 2008