065967/EU XXIV.GP
Eingelangt am 01/12/11

COUNCIL OF
THE EUROPEAN UNION

**Brussels, 1 December 2011**

**17745/11**

**LIMITE**

**CSC 82**
**CSCI 22**

**NOTE**

| | |
|---|---|
| from: | Council Security Committee (Information Assurance) |
| to: | Council Security Committee |
| Subject: | Information Assurance Security Guidelines on User Generated Passwords and Password Management |

1. The Committee will find attached Information Assurance Security Guidelines on User Generated Passwords and Password Management (IASG BP-08) for endorsement.

2. While the attached guidelines apply to communication and information systems handling EUCI, it may also constitute a reference for user generated passwords and password management in systems handling sensitive unclassified information.

This page is intentionally left blank

# IA Security Guideline

User generated passwords and password management

**IASG BP-08**

## I. INTRODUCTION

1. These guidelines, agreed by the Council Security Committee in accordance with article 6(2) of the Council Security Rules (hereinafter CSR[1]), are designed to support implementation of the CSR.

2. These guidelines offer best practices for user generated passwords for access to CIS handling EUCI, in terms of requirements, construction, security and management[2].

3. The Council and the General Secretariat of the Council (GSC) will apply these security guidelines in their structures and communication and information systems (CIS).

4. When EU classified information is handled in national structures, including national CIS, the Member States will use these security guidelines as a benchmark.

5. EU agencies and bodies established under Title V, Chapter 2, of the Treaty on European Union (TEU), EUROPOL and EUROJUST should use these guidelines as a reference for implementing security rules in their own structures.

## II. IDENTIFICATION & AUTHENTICATION

6. An Identification & Authentication (Id&A) system identifies and authenticates users; it does not in itself control access. The user's identity and authenticity is usually the basis for access control. In principle users who cannot be identified are denied access.

7. The Id&A system works as a filter and should be user-friendly and effective, and its strength commensurate with the assessed level of risk.

8. Id&A is a two-stage process: first, potential users assert their identity; second, that identity is verified by the system or part of the system using an authentication process.

9. Id&A mechanisms are based upon one or more of the following "Authenticators":

[1] Council Decision 2011/292/EU of 31 March 2011 on the security rules for protecting EU classified information (OJ l 141, 27.05.2011, p.17).

[2] National Institute for Standards and Technology (NIST) Special publication 800-118 "Guide to Enterprise Password Management" was used as reference.

(a) Id&A by Knowledge - something the user knows, i.e. a secret memory sequence such as a password;

(b) Id&A by Possession - something the user possesses, such as a swipe or a smart card (also referred to as a token);

(c) Id&A by Characteristic - something a user is, i.e. a biometric characteristic such as a fingerprint, a retina or a voice pattern.

10. The initial system risk assessment process should identify which type of system is required and state the requirement for the type (and strength) of the Id&A process in the System-specific Security Requirement Statement (SSRS).

11. This document relates solely to Id&A by Knowledge. For the purpose of this document any knowledge used for authentication is called a password.

12. In general, passwords can either be created by the user or be randomly generated. Each method, whether directly generated by the GSC systems account administrator or indirectly via a token (e.g. as part of a challenge response sequence) has both advantages and disadvantages. Whilst machine generated passwords appear more secure, they are potentially less easy to memorise by users. On the other hand, a user generated password although more easily memorised, can be easier to break. As with determining the type of Id&A system to be employed, the risk assessment process will specify which type of password generation method is required in addition to the length, complexity and the frequency of change.

## III. RECOMMENDATIONS

### General Recommendations

13. User accounts which do not require user interaction and are not locked (i.e. service accounts) should use long randomly generated passwords.

14. In principle, all system-level passwords (e.g. root, enable, system administration, application administration accounts, etc.) should generally be changed at least every three months, ideally every month.

15. In principle, all user-level passwords (e.g. desktop, e-mail, web/Intranet etc.) should be changed at least every six months, ideally every three months.

16. User accounts that have system-level privileges granted through group membership or programs must have a unique password distinct from all other accounts held by that user.

17. Passwords should not be communicated to the end user by non-secure e-mail or telephone.

**Password Construction**

18. Experience has shown that user-chosen passwords are often real words and therefore susceptible to a simple "dictionary attack".

19. Where user-chosen passwords are used, rules should be put in place (preferably enforced by automated means) to prevent passwords being based on the following:

(a) Dates with which the user could be personally associated (e.g. birthdays);
(b) Family names, initials or car registration numbers;
(c) Words found in a dictionary in any language (including inverted words);
(d) Organisation names, identifiers or references;
(e) Telephone numbers or similar all-numeric groups;
(f) User ID (UID), user name, group ID or other system identifier or job-related title (e.g.SYSMAN, INFOSEC);
(g) Any other guessable personal characteristic (e.g. address, nickname, favourite football team, etc.) ;
(h) Any of the above spelt backwards;
(i) Contain more than two consecutive identical characters;
(j) Special characters at the beginning and/or end;
(k) Numbers in sequence at the beginning and/or end.

20. An effective password is a compromise between length, randomness, complexity and the user's ability to remember it. Well constructed passwords may have some or all of the following characteristics:

(a) Contain both upper and lower case characters;
(b) Contain both letters and digits (alphanumeric);
(c) Contain Special Characters where the system permits[3] (e.g. !@#%&=)

[3] Use of special characters is not advisable for certain applications, (e.g. bios passwords) or certain environments. The user documentation for each system should indicate whether or not special characters may be used, even if the system is accessed with different keyboards.

(d) Comprise of at least twelve alphanumeric characters (though the system risk assessment process will determine the minimum required password length)[4]

21. Users must not reuse a previous password. Adding a alphanumeric prefix or suffix to an existing password is not sufficient.

22. Using a "pass-phrase" is another way of generating a pseudo-random password. In some systems the "pass-phrase" can be used on the logon screen. However, most systems only have space to type a password. In this case the actual password can be generated from an easy to remember "pass-phrase". The "pass-phrase" can be based on the words from a book or song or on a statement that the user is unlikely to forget. All guidelines above that apply to passwords also apply to "pass-phrases". An example of a password developed from a phrase:

" I rode my Bicycle 19 kilometres to Brussels & back Last Sunday morning
IrmB19ktB&bLSm " (NB: Do not use this example)

**Password Security and Management**

23. When combined with a UID, passwords can be viewed as an entry key to the system. Therefore passwords should be protected in a manner commensurate with the classification of the system to which they provide access. The following principles should be followed:

(a) A password must not be revealed to anyone other than the legitimate user;

(b) Users should avoid being seen entering their password;

(c) Passwords must not be written down, stored or sent in clear through any system (e.g. IOLAN) or media (e.g. paper files, USB keys)[5].

(d) In principle, user passwords must not be shared with colleagues or managers.

(e) Users should never use the "Remember Password" feature of applications (e.g. within the mail tool or web browser);

(f) If an account or password is suspected to have been compromised all passwords

[4] Minimum 15 characters for user accounts with elevated permissions.

[5] Some GSC departments (e.g. Classified Information Office - BIC) use a significant number of password protected systems on a daily basis. In this case it is acceptable to write passwords down as long as the paper files in question are not marked as such, are kept in their respective premises at all times and are securely put away when not in use (e.g. safe). In cases where emergency access to CIS is necessary, passwords should be kept in a double envelope, preferably with "tamper evident seals", in approved secure furniture (the outer envelope should not identify the nature of the contents, merely those entitled to open it).

related to that person must be changed;

(g) The same password must not be used on different systems.

**System Security Administration**

24. The following guidance should be taken into consideration by system security administrators when developing and implementing a system password policy:

(a) The system should be configured in such a way that temporary or new user passwords have to be changed at the first logon[6];

(b) Passwords should not be displayed on screens when being entered;

(c) Minimum password length should be enforced;

(d) Minimum complexity should be enforced;

(e) It is recommended that the system should be configured to warn the user when a password is due to expire. When the password expires access to the account should be suspended until a new password is set;

(f) The system should be configured to prevent the reuse of the user's previous five passwords or derivatives thereof (i.e. the addition of a numeric prefix or suffix);

(g) The system should be configured to lock the user account after a small preset number of consecutive unsuccessful login attempts[7];

(h) It is recommended that on logon, users are presented with the date/time of their last login and of any unsuccessful attempts to login using their User ID (UID). Users should be instructed to report apparent anomalies such as successful logins not attributable to themselves or unexplained unsuccessful login attempts;

(i) Assuming "password hashing" is used, periodic running of a password cracking program against the password hash file is recommended. Where such programs have not been evaluated, by a reliable source, they must be run on an isolated system, in an auditable and controlled way, with the password file copied across using an air gap (e.g. via a USB drive). Such a program should not however display the "failed" password nor the reason why it failed to the administrators; merely presenting a list of

[6] If a newly generated password has not been changed within a preset period of time, the password should expire at the end of this period.

[7] Accounts can be set to automatically unlock after a set period or preferably, can only be unlocked by the system security administrator. The decision how to unlock an account should be taken as part of the initial risk assessment for the system in question. Using a system security administrator to unlock accounts is probably more secure than allowing the account to be reactivated automatically after a set time period. However, the knowledge that accounts on a specific system can only be unlocked by the system security administrator could be used by an attacker to help facilitate a denial of service attack against the system.

UIDs[8];

(j) The system security administrators should regularly test that the passwords used on the system comply with the system's password policy as required by the SSRS.

(k) Only the strongest methods available to the OS should be employed for the protection of passwords. This applies to the storage of passwords as well as the network authentication mechanism.

(l) Randomly generated passwords should be used during account creation and password reset procedures.

(m) Newly generated passwords should be delivered to the user in such a way that its confidentiality is guaranteed.

[8] If it is decided to run a password cracking programme it is important to decide what action will be taken when a weak password is found. It is suggested that the use of such programme should be pre-announced to the system users. The process of dealing with accounts which are found to have weak passwords should also be communicated to the users.