COUNCIL OF THE EUROPEAN UNION

Brussels, 9 December 2013

17547/13

CSCI 70
CSC 180

NOTE

From :	The General Secretariat
To :	Delegations
Subject :	Information Assurance Security Guidelines on Access Control

1. The Council Decision on the security rules for protecting EU classified information[1] states that "The Security Committee may agree at its level security guidelines to supplement or support this Decision and any security policies approved by the Council." (cf. Article 6(2)).

2. The Council Security Committee approved the attached Information Assurance Security Guidelines on Access Control on the 6 December 2013, CoB.

[1] Council Decision 2013/488/EU of 23 September 2013, OJ L 274, 15.10.2013, p.1

This page intentionally left blank

IA Security Guidelines on Access Control

***IASG* 5-04**

I. PURPOSE AND SCOPE

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

2. This document describes minimum standards to be observed for the purpose of access control to communication and information systems (CIS), for protecting EU classified information (EUCI) in terms of confidentiality, integrity, availability and, where appropriate, authenticity and non-repudiation.

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 TEU, Europol and Eurojust should use these security guidelines as a reference for implementing security rules in their own structures.

6. Access control is understood to be the entire set of technical and procedural measures needed to allow access to CIS and/or the data processed by CIS based on the role and profile defined for the person or service which is handling the data in a CIS, while preventing unauthorised access. Such measures have to be robust to a degree commensurate with the protection needs of the data in question, without becoming a hindrance to the ease of use and availability of the information processed by the CIS.

7. Access control is used to restrict access to assets which can be information, physical objects such as buildings, rooms, passageways etc., as well as to restrict logical access to services and structures, e.g. E-mail, printing and file storage, a workstation, the telephone system, a particular CIS or a set of services of a CIS.

II. ACCOUNT MANAGEMENT

8. Access control is achieved by issuing an account to the client to which access is to be granted or revoked. Accounts can belong to any of the following "clients":

   (a) a person;

   (b) a group of persons - e.g. a "role", "post", or team, the members of which use the account;

   (c) an automatic device - e.g. a robotic loader which can enter e.g. a store to place or retrieve goods;

   (d) a CIS[2];

   (e) a service of a CIS - e.g. an account used to start or run a service or an application;

   (f) an active component of a CIS - e.g. a workstation or network device;

   (g) a group of such components;

   (h) any logical structure which needs to access other logical structures.

   Except for (personal) accounts of type (a) all other accounts are called anonymous accounts
   Accounts of type (b) can also be called generic or functional accounts.
   Accounts of type (e) can also be termed application accounts.
   Examples of type (f) are accounts of Windows workstations in Active Directory domains.
   Examples of types (g) and (h) are accounts of Windows domains in other domains: 'trust' accounts created to allow an account authenticated in one domain to access the resources of the other domain.

9. Access to physical objects can be granted or revoked only on physical access control accounts belonging to (a), (b), or exceptionally to (c), for example to automatic devices which can act independently to move between physical spaces. Accounts for logical access to information assets and CIS is typically applied only to clients of the types (d) - (h), although they can be created for all the clients mentioned (e.g. (c) can be an automatic loader/unloader in a warehouse housing classified items, which loader can receive commands from a computer system and register goods it has successfully moved in a database).

---

[2] In this document, the term CIS covers the set of hardware and software components which runs applications (customised layered products or custom code) providing services to clients. CIS are housed in core and remote hardware, interconnected using network devices and cabling to components such as workstations and/or to other CIS. CIS components are located inside facilities - administrative or secured areas as required by the classification level of the EUCI handled.

10. Logical access control is typically implemented through access control lists (ACLs) and by granting/revoking access rights and privileges.

- Rights are typically read, write and execute to logical assets to which ACLs can be assigned. The right to delete is equivalent to the right to write to a higher level 'folder' or directory.

- Privileges are specific to the operating system or layered product in which the account is used. Privileges often permit the account holder to modify the functional and physical behaviour of a CIS e.g. by changing system time or adding or removing accounts, as well as modify the work of others.

11. Accounts which can change system settings or modify the work of other accounts are called privileged.

12. For access control to succeed, the entity owning the accessed assets must exercise strict account management. Account management includes the steps required for creation, activation, modification, deactivation (disabling) and deletion of accounts.

13. Account management requires that

(a) personal accounts are created only upon request and after suitable authorisation, e.g. in the case of new personal accounts, by the administration of the account owner (user) and by the owner(s) of the assets **(**e.g. information, facilities, CIS, services) to which access is being requested;

(b) the owner of every account must be identified and the details registered along with the account-specific properties (registration);

(c) the access rights and privileges of the account must be kept to the minimum required for the performance of the tasks assigned to the account;

(d) unneeded accounts must be disabled and/or their access rights revoked when the client no longer requires them[3]; should the account be retained but rights and privileges revoked, new rights and privileges must be granted only upon renewed request of the new

[3] e.g. because of termination of employment or change of assignment of a user

administration of the client (if applicable) and the owner of the assets;

(e) in the case of forced termination of employment of a person, that person's personal accounts must be disabled pending further decision to delete them as in 33(b) and the passwords and other authentication methods which the person used to access any non-personal accounts changed or revoked, especially when such accounts are privileged;

(f) anonymous accounts must be kept to an absolute minimum and must also have an owner or sponsor, the sponsor and her/his line management must arrange for a substitute to be named upon changing assignment. If they are not required continuously, these types of accounts should be permanently disabled, activated only when needed and disabled when no longer required;

(g) interactive use of anonymous accounts must be prohibited where technically possible; when such accounts are used interactively, an audit trail shall be generated recording who is using them, when and for which purpose;

(h) membership of privileged groups and the number of privileged accounts must be kept to a minimum;

(i) a temporary account must be created when any internal or external client does not need access to the asset throughout its expected lifetime;

(j) accounts belonging to clients external to the entity owning the accessed assets, often called 'third party accounts', must have an internal sponsor - a physical person responsible for the security of the assets to which access is being requested; third party accounts must be temporary and have a lifetime as set out below; if an external client needs access longer than 12 months, the request for the account must be resubmitted ahead of its planned expiry date by the internal sponsor; and

(k) new temporary accounts must have a lifetime limited to the period for which the client needs it, but at most 12 months; they must be disabled after this period.

14. The creation of a physical access control account (badge) for a person requires the security service to identify the person for whom access is being requested and upon request by the administration, create an account granting access only to the assets which the client shall need to access.

15. Similarly, issuing an account for access to logical assets to a client requires the permission of the owner responsible for the security of the assets, irrespective of whether the account is for a physical person, a CIS, a component of the CIS or a service thereof. While every account must have an owner as required by paragraph 13(f), a logical account need not be a personal user account but can be a structure within the account database[4] such as an application (service) account, a group of persons, a 'domain' consisting of computer, application and user accounts, groups of servers, groups of workstations, etc.

[4] e.g. Active Directory, LDAP

III. ACCESS CONTROL

16. Access control involves the definition of types to be used as well as details of implementation, defence, auditing and maintenance of the access control solution.

Types

17. Three types of access control are commonly defined:

    (a) Mandatory access control (MAC) refers to a type of access control by an overarching command system, e.g. the operating system, which controls access to the information and cannot be overridden for individual clients. MAC is typically decided by the configuration of the CIS or set of CIS. MAC is also imposed by boundary protection solutions[5]. MAC must be used in a multilevel security CIS or set of CIS, when it is required to use client-independent security models e.g. Bell-La Padula, BIBA or Clark Wilson.

    (b) Discretionary Access Control (DAC) is an access control system using users, groups, and read-write-execute permissions where the owner controls who has access to the information according to the need to know principle (NTK).

    (c) Role-based (RBAC) access is assigned to accounts based on the function they have, or the role they play in the organization and is similar to DAC (b) except that individual accounts are never given access rights and privileges but must be assigned to groups to which such authorisation is granted. RBAC is claimed to minimise administrative cost and complexity.

18. These guidelines deal only with RBAC and DAC, which permit fine-tuning of access rights of the clients to services via ACLs and sets of privileges.

Implementation

19. Access control is implemented in a number of processes usually divided into Registration, Identification and Authentication, Authorization, as well as Accountability.

[5] e.g.: pre-configured devices such as diodes: used to prevent backflow of information from CIS of higher classification to an interconnected CIS of lower classification while allowing information flow from the low to the high level.

Registration

20. The registration step involves identifying the client which shall use the account being created. This step requires identification of the account owner e.g. a personnel number, passport or national identity card. The details of the account are then created in the account database of the access control system.

Identification and Authentication

21. When the account attempts to obtain access to assets, the access control process must include a method to uniquely identify the client and confirm that the client is authentic. Typically the account name is presented to the access control system after which one or more authentication methods are used to confirm the identity of the client.

22. Authentication methods can be of the type "something you know", e.g. password or code, "something you have" e.g. a hardware token, "something you are" i.e. biometrics.

23. For access to any classified assets, strong or "two factor" authentication using two (or more) different authentication methods is the minimum requirement. Combining "two-factor" physical and logical access methods should be used for access to assets with classification levels of C-UE/EU-C and above.

Authorisation

24. Following identification of the client and registration, the account is created and given rights and privileges as requested according to the DAC / RBAC method using account management process described above.

25. These rights and privileges grant or prevent access the assets which can be, in the case of CIS, a set of boundary protection and data separation methods or, in the case of physical assets, automatic locks giving access to the facilities or manual opening of doors by security officers of the facilities.

Accountability

26. The access control system must generate audit trails as described in the section on auditing.

Defence

27. Access control systems are a primary target of all attackers. The account database is a concentrated collection of points of entry to the assets which the access control system guards. Attackers gaining access to even unprivileged accounts can use the access thus obtained to gather further information and attack higher level accounts and/or other assets.

28. Prior to the deployment of an access control solution, the threat scenario to which it is exposed must be estimated by a preliminary risk assessment, following which the solution being (re)designed needs to be subjected to a detailed risk assessment and accredited as required before being released for use.
    The security measures implemented must minimise the impact of attack and contain the damage while recording events in a way which enables identification of perpetrators for subsequent disciplinary and/or legal action. The information collected must also trigger a review of the access control mechanisms to prevent recurrence.

29. While minimising the inconvenience to the account holder, defence mechanisms must be deployed in a measure commensurate to the sensitivity of the accessed assets and the level of risk considered acceptable by the asset owners (risk appetite).

Auditing

30. Access control systems must be audited (monitored) continuously to ensure that accounts are being properly managed.

31. Processes and procedures must be implemented to monitor use and abuse of the access control mechanism and to detect abuse or malfunction of accounts (intrusion detection in the case of logical assets, intruder detection in the case of physical assets).

32. Within the limits imposed by applicable laws, regulations and security operating procedures, access control systems must include monitoring and recording of successful and failed access via automated or manual logging, generating an audit trail.

33. Procedures or automatic processes must be in place to detect unused accounts:

(a) unused accounts must be disabled after a set grace period;

(b) within the limits of legal or regulatory requirements, accounts which are unused for a predetermined (longer) grace period must be deleted**.** Prior to deleting an account, every effort is made to contact the account owner. In case of non-responsiveness by the owner, the owner's administration must be contacted to check whether there is a need for assets owned by and accessible only to the account (e.g. personal folders). In this case the administration must ask that such assets are made accessible to designated accounts which have a need to know;

(c) auditing of temporary accounts must be in place using either organisational or automatic processes and procedures; the audit trail shall record at whose request, for whom, for which purpose and when such accounts were created, disabled or deleted; auditing must also confirm the successful disabling of temporary accounts after they are no longer needed; and

(d) the membership, rights and privileges of third party, group and anonymous accounts must be reviewed periodically, as a minimum every 12 months, e.g. to determine whether all members need to be part of the account and whether the account and/or its rights are needed.

34. Accounts suspected of being compromised should be immediately disabled after estimating the impact of disabling the account and obtaining the consensus of the Information Assurance Operational Authority (IAOA) and the CIS business owner(s).

35. The alerts and records generated by the auditing systems must be reviewed regularly. Alerts should result in notifications being sent to the security event monitoring process.

36. Unusual events must be initially considered to be security breaches until proven otherwise. An investigation must be started by suitably qualified experts to establish whether a security incident has happened. If it cannot be determined what the cause of the anomaly was or if a security incident is confirmed, a security incident handling process is started to determining the nature of the disturbance, its impact, its cause and if applicable the perpetrator(s), as well as to initiate business continuity and/or service restoration measures if needed.

37. The results of such investigation shall be reported to the IAOA and Security Accreditation

Authority (SAA) of the system for corrective action and, if applicable, to the administration for disciplinary action against perpetrators.

Maintenance

38. The operational procedures of access control systems must include procedures and automatic processes to monitor external and internal sources of information about potential vulnerabilities, weaknesses and misconfigurations of the access control mechanism.

39. The suitability and validity of the implemented access control systems must be reviewed by the owners of the assets accessed after incidents and at regular intervals in the absence of incidents, typically every 12 months, to determine the need for modification or replacement of the system.

IV. TERMS AND DEFINITIONS

Asset	Asset means anything that is of value to an organisation, its business operations and their continuity, including information resources that support the organisation's mission. Assets can be information, a CIS handling information, components of a CIS, services offered by the CIS, or facilities housing any of these.
Client	A client can be a physical person, another CIS, a component thereof, or another "service" inside a CIS. In the context of logical access, a client accesses services offered by a CIS to input, process or retrieve information. A client is sometimes termed the "subject" e.g. in the context of public key infrastructure (PKI). In the context of physical access, the client accesses facilities.
Facilities	Buildings, passages and rooms.
Owner	The owner of an account is the user of a personal account, or the physical person responsible for anonymous accounts such as service (application) or group accounts.
Service	In this document the term service refers to a particular information processing functionality provided to authorised and authenticated clients by all or part of a CIS - e.g. e-mail, instant messaging, printing, database, web, file transfer, enterprise resource planning, document management, authentication and authorisation (LDAP, active directory) etc. The term as used here does not cover built-in memory-resident modules or executables which form part of the operating system or layered product itself (e.g. the Event Log service of Microsoft Windows). A service is sometimes termed a "resource" or an "object" e.g. in the context of public key infrastructure (PKI).