EUROPEAN
COMMISSION

Brussels, 22.3.2019
C(2019) 2344 final

IT security standard

Access control and authentication

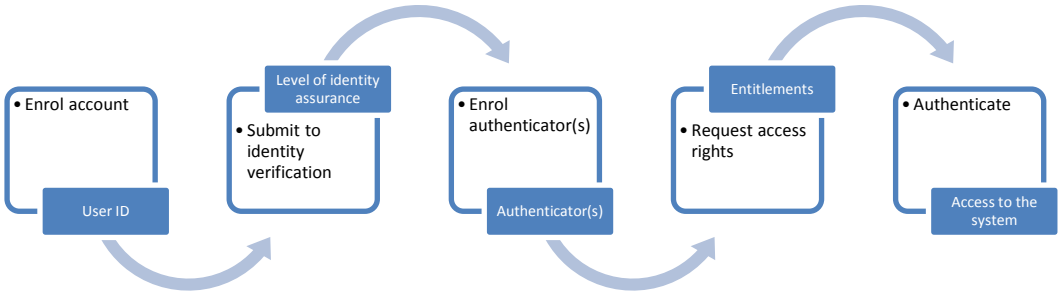
CONTENTS

1. INTRODUCTION

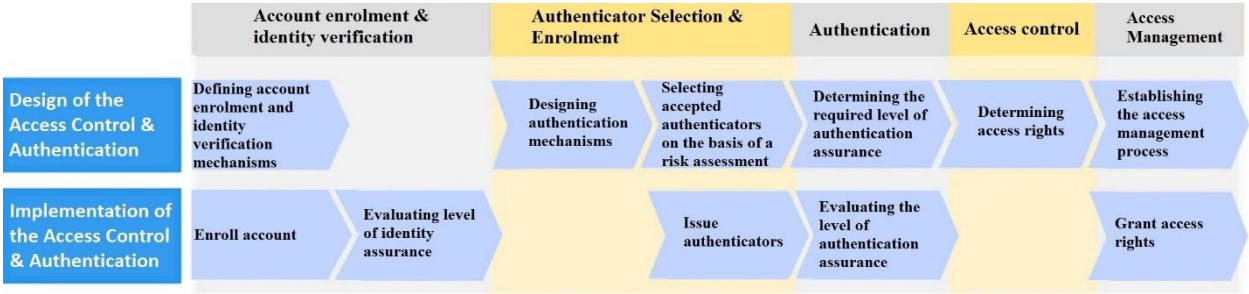
In accordance with Commission Decision (EU, Euratom) 2017/46[1] and Commission Decision (EU, Euratom) 2017/8841 (its Implementing Rules), and in particular Article 12, the access control and authentication standard relating to Commission Decision C(2006) 3602 should be repealed.

This standard on access control and authentication establishes security requirements and covers the following main activities, which are further defined in the various sections below:

Access control and authentication from a user perspective



Access control and authentication from a system owner perspective



2. PURPOSE

This security standard establishes:

- minimal requirements for access control and authentication on IT systems;
- requirements for setting and issuing authenticators;
- requirements applying to user access management processes; and
- roles and responsibilities in the management of access control.

3. SCOPE

This document sets out minimum requirements applying to all applications and IT systems hosted on Commission premises. Some are mandatory and subject to compliance verification. Some are in the form of recommendations (i.e. guidance) based on market best practices, and not

[1] Commission Decision (EU, Euratom) 2017/46 of 10 January 2017 on the security of communication and information systems in the European Commission (OJ L 6, 11.1.2017, p. 40).

ken.ducatel@ec.europa.eu

subject to compliance verification. These may become mandatory in future versions of this standard, in the light of customer feedback, further best practice and compliance analysis.

4. EXCEPTIONS

This security standard is mandatory and an integral part of the Commission's information security policy. Exceptions must be handled in accordance with Article 8.3.d.iv of Commission Decision (EU, Euratom) 2017/8841.

5. DEFINITIONS

For the purposes of this standard, in addition to the definitions in Article 2 of Decision (EU, Euratom) 2017/46 and Article 2 of Commission Decision (EU, Euratom) 2017/8841, the following definitions also apply:

TERM	DEFINITION
account	A collection of data associated with a specific user, token or computer known by the information system, set up in order to identify a user.
adaptive authentication	A combination of variables (users' behaviour, devices they use and other variables) results in a risk profile. Adaptive authentication is a method for selecting the right authentication factors, depending on that risk profile and tendencies, i.e. for adapting the type of authentication to the situation. Authentication is influenced by the risk context of the authentication attempt.
application administrators	Application administrators are persons that play a critical role in keeping the applications that the organisation relies on running. They install, update, tune, diagnose and manage both internal and third-party applications.
authenticator or authentication factor	A category of credential used for authenticating. There are three main authentication factors: – the knowledge factor – a category of credentials consisting of information that the user knows, such as a personal identification number (PIN), a password or the answer to a secret question; – the possession factor – a category of credentials based on items that the user has with him/her, typically a secure hardware device such as a security token or a mobile phone used in conjunction with a software token; and – the inherence factor – a category of credentials consisting of elements that are integral to the individual in question, in the form of biometric data.
authentication service provider	Aims to provide authentication services for systems of all or some of the European institutions and bodies. It authenticates users and hands over their identity to business applications.
authorisation	Phase during access when it is verified that the requester (requesting user) is entitled to the requested access to the information system resource.
authoritative source	Any source, irrespective of its form, that can be relied on to provide accurate data, information and/or evidence that can be used to prove a person's identity.
eIDAS	Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (the eIDAS Regulation) has been fully in force since 1 July 2016.

ken.ducatel@ec.europa.eu

entitlement	When a user is entitled to certain privileges or he/she has certain access rights.
identity	Set of characteristics that allow a CIS to distinguish one entity (or individual) from all others in a specific group.
privileged account	An account that holds privileges, e.g. a device's or operating system's local and domain administration accounts, a database's or network device's administration accounts. It provides greater access and requires additional authorisation.
sensitive non-classified information	Information (as defined in Commission Decision (EU, Euratom) 2015/443) that the Commission is obliged to protect under the Treaties or acts adopted to implement them.
service account	An account used by an automated service, not an individual user.
system administrators	Persons responsible for the upkeep, configuration and reliable operation of computer systems, especially multi-user computers such as servers.
two-factor or multi-factor authentication	A combination of two (or more) authenticators that are vulnerable to attack involving two (or more) vectors (e.g. combining the knowledge factor and the possession factor requires an attacker to phish a secret and steal an item).
two-step authentication	A combination of two authenticators that are vulnerable to attack involving twice the same vector (e.g. malware infection).
user account	An account that has a single individual owner.
userID	User identifier – a character string used as a unique name for an account.
vector of attack	Technique by means of which a malicious user can gain unauthorised access to a device, application, database or the network.

6. ACCOUNT ENROLMENT AND IDENTITY VERIFICATION

Set out below are the minimum definitions and provisions required for identities in order to help the system owner assign the appropriate identity assurance levels.

6.1. Defining account enrolment and identity verification mechanisms — enrol account

(M=mandatory, R=recommended)

SN	Requirement	Implementation
1.	A user's identity **shall** be composed of at least: – current family name; – current first name(s); and – personal e-mail address.	M
2.	The system owner **should** collect additional information about the user in order to verify her/his identity, such as the phone number and some corporate properties.	R
3.	The system owner **shall** verify that the personal email address and the additional properties are correct before creating an identity.	M
4.	The system owner **should** maintain a record, including audit logs, of all the steps taken to verify the identity of the applicant.	R

ken.ducatel@ec.europa.eu

5.	Each account **shall** be linked to a unique userID. Each userID **shall** be unique and **shall not** be re-assigned to another person. One identity may have different accounts based on the business needs.	M

6.2. Evaluating level of identity assurance

(M=mandatory, R=recommended)

SN	Requirement	Implementation
6.	A level of identity assurance **shall** result from the verification of the applicant's identity.	M
6.a	– The level of identity assurance **shall** be established on the basis of the verifications performed and reflect the risk of the verifications failing to confirm the real-world existence of the applicant's claimed identity.	M
6.b	– The level of identity assurance **shall** have one of the following values[2]: o **basic** – limited assurance as to the identity of a user; o **medium** – assurance is obtained through verification of the user identity on the basis of additional controls that reduce the risk of misuse or alteration of identity; or o **high** – assurance is obtained through verification of the user identity on the basis of formal controls that are more stringent than 'medium' controls and exclude misuse or alteration of identity.	M
7.	The identity assurance level of an applicant **shall** be verified prior to allocating authenticators to the user.	M

7. AUTHENTICATOR SELECTION AND ISSUANCE

7.1. Designing authentication mechanisms

(M=mandatory, R=recommended)

SN	Requirement	Implementation
8.	Every account that grants access to IT systems **shall** be linked to at least one authenticator. Access to the IT system **shall** be granted on the basis of a combination of a userID and authenticator(s).	M
9.	The authenticator **shall** consist at least of a password that complies with the password technical standard.	M
10.	The account **should** be linked to additional authenticators.	R

[2] Annex I, section A gives some guidance and clarifications on the different levels of identity assurance.

7.2. Selecting accepted authenticators on the basis of a risk assessment

(M=mandatory, R=recommended)

SN	Requirement	Implementation
11.	The selection of additional authenticators **shall not** undermine the security of the primary authenticator.	M
12.	Two-factor (or multi-factor) authentication **shall** meet the following requirements: – authentication factors used in combination **shall not** be vulnerable to a single attack vector; – a breach of one authentication factor **shall not** compromise the confidentiality or integrity of the other; and – at least one of the authentication factors **should** be non-reusable and non-replicable.	M
13.	An inherence authentication factor **shall** always be used in combination with a knowledge or a possession factor.	M

7.3. Issue authenticators

(M=mandatory, R=recommended)

SN	Requirement	Implementation
14.	The process of issuing authenticators **shall** provide adequate assurance that they have been delivered to the intended recipient, depending on the level of identity assurance obtained: – **basic** – the system owner **shall** determine a delivery mechanism (e.g. e-mail) that can be assumed to reach only the intended person; – **medium** – the system owner **shall** determine a delivery mechanism, through a side channel that was not used as part of the identity verification process, that can be assumed to reach only the person to whom the authenticator belongs; – **high** – the system owner **shall** determine a delivery mechanism that verifies that the authenticator is delivered in person to the individual to whom it belongs (e.g. badge).	M
15.	The process of renewing authenticators **shall** provide the same level of assurance as the initial issuing.	M

8. AUTHENTICATION

8.1. Determining the required level of authentication assurance

(M=mandatory, R=recommended)

SN	Requirement	Implementation
16.	Each authentication attempt **shall** be assigned a level of authentication assurance representing the degree of confidence that the person using the authenticators is the legitimate owner of the user account.	M

17.	The level of authentication assurance **shall** be based on the type and combination of authenticators used and the level of identity assurance, as follows[3]: – **basic** – a single authenticator is used or authenticators meet eIDAS technical requirements for a low level of assurance[4]; – **medium** – two-step authentication is used or authenticators meet eIDAS technical requirements for a substantial level of assurance; or – **high** – two-factor authentication is used or authenticators meet eIDAS technical requirements for a high level of assurance (e.g. certificate-based authentication).	M
18.	The level of authentication assurance **shall** never receive a value that exceeds the level of identity assurance associated with an account[5].	M
19.	Users **should** be able to set a minimum level of authentication assurance for their account but this level must not be below the level determined by the system owner.	R

8.2. Context-based risk adjustment of the level of authentication assurance

(M=mandatory, R=recommended)

SN	Requirement	Implement ation
20.	The level of authentication assurance **should** be influenced by the risk context of the authentication attempt (adaptive authentication).	R

8.3. Evaluating the level of authentication assurance

(M=mandatory, R=recommended)

SN	Requirement	Implement ation
21.	The system owner **shall** determine the level of authentication assurance required for its system to accept an authentication request, on the basis of a risk assessment.	M
22.	That required level **shall** have one of the following values: – **basic** – any supplied level of authentication assurance is acceptable; – **medium** – a high or medium level of authentication assurance **shall** be acceptable; or – **high** – a high level of authentication assurance **shall** be acceptable.	M
23.	The system owner **shall** ensure a high level of authentication assurance for sensitive non-classified information or operations.	M

[3] Annex II provides a table to clarify the different levels of authentication assurance.

[4] Annex I, section B provides a table with the eIDAS technical requirements.

[5] For example, if a user authenticates with two factors (for high-level authentication assurance), but obtained only a basic level of identity assurance on enrolment, the level of authentication assurance supplied to the system will not exceed 'basic'.

ken.ducatel@ec.europa.eu

9. ACCESS CONTROL

9.1. Determining access rights

(M=mandatory, R=recommended)

SN	Requirement	Implement ation
24.	Access to system functionalities and data **shall** be restricted to authorised users on the basis of the 'need to know' principle.	M
25.	Authorisation mechanisms[6] in the system **shall** ensure that access is: – automatically denied unless accounts have been explicitly authorised for the system; and – automatically restricted to access rights granted to the account.	M
26.	The system owner **shall** determine access rights associated with differentiated levels of authorisation to access the system data and functionalities.	M
27.	The access rights **shall** be determined on the basis of a risk assessment that considers at least: – information sensitivity and level of classification – the need to limit access to system data, in line with data classification, general data sensitivity and applicable regulation; and – business process controls and incompatible duties – the need to limit access to system functionalities to ensure segregation of incompatible duties or enforce business process controls.	M
28.	Determined access rights **shall** be reviewed periodically to check that they continue to ensure the protection of sensitive non-classified information, the enforcement of process controls and the segregation of incompatible duties.	M
29.	Access decisions (both positive and negative) following a user access request during a login process **shall** be logged in order to provide an audit trail.	M

10. ACCESS MANAGEMENT

10.1. Establishing the access management process

(M=mandatory, R=recommended)

SN	Requirement	Implement ation
30.	Access rights **shall** be inherited on the basis of the attributes of an account or granted, on formal request, specifically to the account. Granted access rights constitute the entitlements of an account.	M
31.	Where access rights are granted on request, the system owner **shall** grant them only if: – the request has been approved at the proper business level; – where the rights grant access to sensitive non-classified information, the request has been approved by the data owner or their authorised representative; – the user has provided valid business justification and specified the purpose(s) for which they need the information; and	M

6 Authorisation mechanisms may build on the corporate properties of the user account (e.g. properties of the user account in central databases).

	– the verification of the business justification is appropriately documented, so as to enable future inspection and audit.	
32.	Segregation of duties **shall** be implemented between user profiles at operating systems, databases, middleware, network devices and infrastructure components, and between 'system administrators' and 'application administrators' profiles.	M
33.	The standard profiles **shall** be implemented on the basis of the 'segregation of duties' principle: – the system owner **shall** identify any incompatible information system functions, which, when held by one person, entail a business risk (lack of segregation of duties); and – incompatible functions **shall not** be accessible by a single person (segregation of duties).	M
34.	The system owner **shall** implement controls to ensure that, where the user's attributes (e.g. job responsibilities) change, user entitlements are re-evaluated for appropriateness.	M
35.	The system owner **shall** implement controls to ensure that a Commission user who no longer has contractual or statutory ties with the Commission is denied access to resources in a timely manner, either by disabling the account or by revoking all authorisations.	M
35.a	– This control **should** be automated;	R
35.b	– All authorisations **should** be revoked, or the account disabled, within 24 hours of the effective user termination time (or date).	R
36.	The System Owner **shall** have procedures to disable accounts in case of a security incident involving those accounts.	M
37.	The system owner **shall** verify periodically that the business justification for all entitlements continues to be valid.	M
37.a	– For systems that require a high level of authentication assurance, this **shall** be done at least annually.	M
37.b	– For all other systems, this **should** be done at least annually.	R
37.c	– Any changes in the corporate properties of a user **should** trigger a review of the access rights.	R

11. PRIVILEGED ACCOUNTS

11.1. General requirements

(M=mandatory, R=recommended)

SN	Requirement	Implementation
38.	Administrative privileges allocated to users **shall** be minimised and granted on a strict and granular 'need to know' basis.	M
39.	Users who perform system administration tasks **shall** have an individual separate account used exclusively for that purpose. This **shall** be the case for the account of any such user on application and content servers, operating systems, databases, middleware, network devices and infrastructure components.	M
40.	Passwords of accounts with system administration privileges **shall** have a lifespan (max. 90 days).	M

41.	If passwords of privileged accounts are not automatically modified after each use (password rotation), authentication **shall** rely on a second independent authenticator, ensuring multi-factor authentication.	M
42.	Privileged accounts **shall** be formally reviewed at least every six months.	M
43.	All requests for administration privileges **shall** be treated in accordance with the rule 32.	M

12. SERVICE ACCOUNTS

12.1. General requirements

(M=mandatory, R=recommended)

SN	Requirement	Implement ation
44.	Service accounts **shall** comply with the following specific requirements in terms of authenticators:	M
44.a	– where accounts are required to perform automated tasks on a system, interactive human login **shall** be eliminated and:	M
44.a.i	○ when designing a system, the system owner **shall** implement mechanisms supporting this principle; and	M
44.a.ii	○ passwords **should** be replaced by authenticators that cannot be memorised or intercepted, such as certificates supported by adequate encryption and key management mechanisms in line with the cryptography and public key infrastructure standard; and	R
44.b	– if passwords are used, this **shall** be based on an evaluation of the risk and formally accepted through the exception procedure. In such cases, stringent password configuration requirements shall be applied that at least meet the requirements for privileged accounts (see section 11) and the requirements of password technical standard for privileged accounts.	M
45.	Service accounts with administrative privileges **shall** be restricted on a granular basis and following strict 'need to know' principles.	M
46.	The system owner **shall** implement appropriate auditing of service accounts activity.	M

13. DEFAULT/GENERIC ACCOUNTS

13.1. General requirements

(M=mandatory, R=recommended)

SN	Requirement	Implement ation
47.	Default/generic (non-nominative) accounts, such as administrator or root and shared accounts, **shall not** be used.	M
48.	However, in exceptional situations, the use of such default/generic accounts can be allowed if no alternative is available; in such cases, a business justification **shall** be filed with the access request and accountability will remain with an individual to whom the account is explicitly assigned.	M

14. IDENTITY & ACCESS MANAGEMENT GOVERNANCE

14.1. General requirements

(M=mandatory, R=recommended)

SN	Requirement	Implement ation
49.	The system owner **shall** be accountable for the implementation of identity and access management mechanisms that comply with the requirements in this standard.	M

14.1. Delegation

(M=mandatory, R=recommended)

SN	Requirement	Implement ation
50.	The system owner **should** delegate the implementation of some or all of the enrolment mechanisms to a Commission authoritative source of identities.	R
51.	Where implementation is delegated to an authoritative source of identities, the system owner **shall**:	M
51.a	– determine which of the applicable requirements established in this standard are implemented at the level of the repository and the supporting processes;	
51.b	– ensure that every requirement that is not implemented at the level of the authoritative source is nevertheless implemented; and	
51.c	– remain accountable for the usage of the authoritative source data in its IT system.	
52.	The system owner **shall** delegate the implementation of all the authentication mechanisms to a Commission authentication service provider for IT systems handling 'sensitive non-classified'[7] data.	M
53.	The system owner **should** delegate the implementation of some or all authentication mechanisms to a Commission authentication service provider for IT systems handling 'publicly available' or 'Commission use'[8] data.	R
54.	Where implementation is delegated to an authentication service provider, the system owner **shall**:	M
54.a	– formally agree with the authentication service provider, for each of the requirements in this standard, which of them is responsible for its implementation;	
54.b	– ensure that any requirement in this standard that is not implemented by the authentication service provider is nevertheless implemented; and	
54.c	– remain accountable for the usage of the authentication service provider's services in the system.	

[7] Previously 'limited high'.
[8] Previously 'public' and 'limited basic'.

ken.ducatel@ec.europa.eu

REFERENCES

[1] eIDAS, Commission Implementing Regulation (EU) 2015/1502 [online]; http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32015R1502&from=EN

[2] eIDAS, *eIDAS LOA guidance — European Commission* [online]; https://ec.europa.eu/cefdigital/wiki/download/attachments/40 044 784/Guidance%20on%20Levels%20of%20Assurance.docx?version=1&modificationDate=1488295895839&api=v2

[3] The Common Criteria, *Common criteria for information technology security evaluation (CC)* [online]; https://www.commoncriteriaportal.org/cc/

[4] Risk Management, IT Security Risk Management Methodology (ITSRM²) [online]; https://webgate.ec.europa.eu/fpfis/wikis/pages/viewpage.action?pageId=222010104

ANNEX I

A. Identity assurance levels

The table below is indicative and illustrates the identity assurance levels. System owners can consult eIDAS Regulation [1] for further elements or details.

Identity level	Elements needed
Basic	Only the existence of the e-mail address is verified during the enrolment process.
Medium	This could include controls equivalent to eIDAS' 'substantial' and 'low' assurance levels, which include at least the following: – the person can be assumed to be in possession of identity evidence recognised by a Member State; – the evidence can be assumed to be genuine and appears to be valid; – it is known from an authoritative source (e.g. a Member State's population register) that the claimed identity exists and it may be assumed that the person claiming the identity is one and the same.
High	This includes controls equivalent to eIDAS' 'high' level of assurance and checks by the Commission's Directorate-General for Human Resources when recruiting.

B. Authentication mechanism

The table below focuses on the threats associated with the use of the authentication mechanism and lists the requirements for each assurance level. In this section, controls are understood to be commensurate to the risks at the given level [2].

The authentication mechanisms used in the authentication phase cannot prevent all attacks completely – they can only offer resistance on a certain level of security/assurance. A standard way to quantify the resistance of different mechanisms is to rank them according their resistance against attacks with a certain attack potential (i.e. strength of an attacker).

The terms 'enhanced-basic', 'moderate' and 'high' in relation to assurance levels denote the different attack potentials. This terminology is borrowed from ISO/IEC 15408 (Information technology — Security techniques — Evaluation criteria for IT security) and ISO/IEC 18045 (Information technology — Security techniques — Methodology for IT security evaluation). The text of the standards is also freely available [3] (CCPART1-3 being equivalent to ISO/IEC 15408 and CEM equivalent to ISO/IEC 18045).

ISO/IEC 15408-1 defines attack potential as a 'measure of the effort to be expended in attacking a [mechanism], expressed in terms of an attacker's expertise, resources and motivation'.

Annex B.4 to ISO/IEC 18045 / CEM contains guidance on how to calculate the attack potential necessary to exploit a given weakness of an authentication mechanism.

ken.ducatel@ec.europa.eu

Assurance level	Elements needed
Low	1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity. *GUIDANCE*: *The release of person identification information is about transmitting the minimum data set (MDS) to the relying party.* 2. Where person identification data is stored as part of the authentication mechanism, it is secured in order to protect against loss and compromise, including analysis offline. *GUIDANCE*: *Stored personal data must be subject to strict access controls. Measures should be taken to protect person identification data, e.g. encryption and hashing in accordance with good practice, such as ENISA algorithms, key sizes and parameters report or national cryptographic guidance.* *All access should be audited.* 3. The authentication mechanism implements security controls to verify the means of electronic identification, so it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with enhanced-basic attack potential can subvert the authentication mechanisms. *GUIDANCE*: *All required verification steps must be clearly described, implemented and tested.*
Substantial	Level low, plus: 1. The release of person identification data is preceded by reliable verification of the electronic identification means and its validity through a dynamic authentication. *GUIDANCE:* *In practice, this means that the authentication means should include a one-time code or one-time challenge-response to ensure that it is truly dynamic. The one-time code or challenge should be generated in such a way that it cannot be tampered with.* *When using random numbers in a challenge-response protocol, care should be taken to ensure their 'quality', e.g. by following good practice for cryptographically secure pseudo-random number generators.* 2. The authentication mechanism implements security controls to verify the means of electronic identification, so it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with moderate attack potential can subvert the authentication mechanisms.
High	Level substantial, plus: – the authentication mechanism implements security controls to verify the means of electronic identification, so it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication mechanisms. *GUIDANCE:* *If cryptography is used to secure an authentication mechanism, strong cryptographic protocols and appropriate key lengths should be selected.* *An important method to ensure the strength of cryptographic protocols are cryptographic analyses, such as cryptographic security proofs.* *Where protocols are known not to be secure (e.g. SSL v3), that should be taken into account, as should any known practical attacks on certain cryptographic protocols and measures put in place to counter any attacks where such protocols are being used.* *Where the authentication mechanism uses a cryptographic solution, not only the cryptographic primitives but also the protocols and the environment, especially key management, should be taken into account.*

ANNEX II

The table below shows the authentication assurance levels, which are a combination of identity assurance levels and authenticators. These are the minimum levels that can be assigned to a userID.

Levels of Authentication Assurance required for a System

AUTHENTICATORS / IDENTITY ASSURANCE LEVELS	SINGLE AUTHENTICATION	TWO-STEP AUTHENTICATION	TWO-FACTOR AUTHENTICATION
BASIC	**BASIC**	**BASIC**	**BASIC**
MEDIUM	**BASIC**	**MEDIUM**	**MEDIUM**
HIGH	**BASIC**	**MEDIUM**	**HIGH**

ken.ducatel@ec.europa.eu