Draft recommendation

Passwords

(and other unshared secrets)

Version submitted for public consultation until December 10th, 2021

This document is a courtesy translation of the original draft recommendation in French. In the event of any inconsistencies between the French version and this English translation, please note that the French version shall prevail.

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Introduction

The Commission nationale de l'informatique et des libertés (CNIL) (hereinafter the “Commission”),

Considering that password authentication is one of the most widespread measures to secure automated processing of personal data;

Noting that the proliferation of computer attacks, which has resulted in the compromise of numerous password databases, results in the improvement of attackers' knowledge on passwords uses;

Noting also that the widespread usage of the same password to connect to different online accounts, and/or of passwords based on public information concerning them (date of birth, children's names, etc.), reinforces the obligation for data controllers to implement all measures to ensure the security of personal data;

Believing necessary, for bringing greater confidence in digital services, to define the technical modalities of this authentication method to provide an appropriate level of security, and to issue recommendations relating to the measures to implement as well as the rules to apply to its usage;

After having discussed both with its European counterparts and with the *Agence nationale de la sécurité des systems d'information* (ANSSI), to propose an update of its technical framework providing a minimum level of security consistent with best practices in security;

Recalling that, in cases where the minimum level of security recommended by this deliberation is insufficient, it will be usefully supplemented by the ANSSI guide entitled “*Recommandations relatives à l’authentification multifacteur et aux mots de passe*”, to determine the necessary security measures;

SUBMITS THE FOLLOWING TEXT FOR CONSULTATION:

I - General Password Security Recommendation

Article 32 of the GDPR requires that controllers and processors implement technical and organizational measures to ensure a level of security consistent with the specific risks that the processing creates in terms protection of personal data. The Commission reminds that these measures must be determined in such a way as to guarantee a level of security adapted to the risks.

In this context, many processing use passwords or other unshared secrets to protect access to the data. In the following, the term “password” designates any knowledge factor[1], i.e. any set of revocable information only known by the data subject and allowing or contributing to his authentication. It includes, in particular, “passphrases” (deemed to be longer than passwords) and unlocking codes, and excludes cryptographic keys and secrets.

The objective of this document is to define the minimum technical and organizational requirements recommended by the CNIL for authentication with a password or any other unshared secret (except for cryptographic keys and secrets) when implemented in the context of a personal data processing.

In general, the Commission recommends that all data controllers guarantee a minimum level of security based, on the one hand, on a sufficient length and complexity, equivalent to an 80 bits of entropy without additional measures and, on the other hand, on implementation and governance rules to ensure password security throughout their life cycle.

Actors can nevertheless implement other security measures than those described in this recommendation if they can demonstrate that they guarantee, at least, an equivalent level of security. In particular, the Commission has always considered that other means of authentication, such as two-factor authentication or electronic certificates, or more secure than passwords.

[1] As a reminder, passwords are one of the three authentication factors defined by the ANSSI and CNIL authentication guide which are: "knowledge factor" (possession of hidden information), "possession factor" (possession of an object, such as a smartcard) and “inherence factor” (biometric characteristic).

In this regard, the risks specific to certain processing operations (for example, in the context of sensitive or large-scale data) or categories of users (for example, IT administrators) may require more stringent measures than those defined in this document, and in particular the implementation of a multi-factor authentication process.

II - On governance

The Commission recommends that any organization using password-based authentication defines a password management policy. Written by the actors in charge of security and IT resources in the organization (like CISO, CIO or DPO), it should be approved by the data controller and communicated to all those concerned.

Data subjects must be made aware of the threats and risks relative to password compromise as well as the behaviour to adopt in case of such event. Training must be adapted to the different audiences considering their skills, their level of responsibility and the sensitivity of the data they will access. Controllers can usefully promote password managers and give information regarding the best practices for their use (e.g. it requires a strong master password and to regularly back up databases).

Finally, any system used in an organization must require a modification of the default passwords at the first connection.

III - On the operational aspects of password authentication

Preamble and definitions

The Commission considers that rules and recommendations described in appendices B1 and B2 of the "*référentiel général de sécurité*"[2] (RGS) are the references to evaluate what is a "renown strong public algorithm". To ensure that "the software implementation is free from known vulnerabilities", the Commission recommends choosing software or software components that are regularly maintained on the security aspects, using only up-to-date versions and monitoring their security.

We call "entropy" the amount of randomness in a system. For a password or a cryptographic key, it corresponds to its unpredictability, and thus to its robustness against brute force attacks. In this recommendation, the term entropy, applied to a password, corresponds to its ideal entropy assuming it is randomly generated. In computer science, entropy is commonly measured in a number of "bits", i.e. as the number of binary digits (equal to either "0" or "1") necessary to contain an equivalent quantity of randomness. Thus, a credit card code with four decimal digits randomly chosen, each with a value between "0" and "9", gives ten thousand possibilities (10 to the power of 4, denoted 10^4). To obtain an equivalent number of binary possibilities, it is necessary to use 13 bits, because 2 to the power of 13 (or 2^{13}) is equal to 8 192, which is of the same order of magnitude as 10^4. We will therefore say that a code of four random decimal digits has an entropy of 13 bits[3].

Any rule for password generation limits the number of possible passwords and, thus, decrease the entropy for a given length. For example, choosing a password among the words of a language greatly limits the number of possible letter combinations. Indeed, each language admits only a limited number of sequences of letters, used to form the syllables of words. The lure to pick "easy-to-remember" passwords facilitates, for many users, the so-called "dictionary" attacks, in which instead of testing all possible passwords only a few are tested, like dictionary words or first names as well as "classic" derivations (for example, from the word "kangaroo" could be derived and tested combinations such as "k4ng4roo", "kangaroo01", "KaNgARoO", etc.).

When users are free to choose passwords that are not strictly random, it is necessary, to maintain a given level of entropy, to define a password management policy prioritizing the length of passwords over complexity, or even, depending on the risks, to increase the targeted entropy of the password policy. Indeed, if we expect users to use dictionary words, it is preferable to impose passwords rules that would lead them to choose a series of words instead of only one. It is recommended to guide them in this choice, by reminding them, in particular, that it is preferable to choose words without any links between them.

[2] https://www.ssi.gouv.fr/administration/reglementation/confiance-numerique/le-referentiel-general-desecurite-rgs/liste-des-documents-constitutifs-du-rgs-v-2-0

[3] The same computations can be applied to letter combinations: 26 possible choices per character for uppercase letters, 52 for uppercase and lowercase letters, 62 if you add numbers, etc.

Users should also be advised to avoid including any personal information (date of birth, first names of relatives, etc.) in their passwords, as these elements would greatly facilitate targeted attacks.

1. Password authentication

When password authentication is carried out through a network connection, and *a fortiori* if the latter is operated by a third party, the Commission recommends that:

- a measure allows the client to control the identity of the authentication server is implemented, through a certificate on the authentication server;
- the communication channel between the authenticated server and the client is encrypted with a secure encryption function (i.e. a renowned strong public algorithm whose implementation is free of known vulnerability);
- enhanced security measures are implemented to guarantee the confidentiality of the private keys used to encrypt the connections;
- passwords never appear in the addresses of remote resources, neither as cleartext nor hashed.

The first three points can be implemented with the TLS protocol in a configuration that respects the corresponding ANSSI recommendations described in its document SDE-NT-35 / ANSSI / SDE / NP1 entitled "*Recommandations de sécurité relatives à TLS*".

Regarding the procedures for password generation for the authentication to an account, the data controller must ensure a sufficient level of security for passwords, for example by requiring minimal size and complexity. It further recommends that the data controller informs in advance individuals using password authentication of the policy implemented and especially of any maximum password size supported.

Apart from unlocking codes (see case n°4), the Commission recommends that as soon as the data controller identifies a risk related to abusive passwords submission (especially when the processing is accessible via the Internet), he or she sets a maximum size for the password fields. The maximum must be large enough to allow the use of phrases as passwords while avoiding denial of service attacks resulting from the processing of an excessively long password. In principle, their maximum size cannot be less than 50 characters for password authentication with or without account restrictions (case n°1 and n°2). As an example, it could be in the order of a few hundred characters.

Finally, to encourage the use of password managers and improve accessibility, the Commission recommends avoiding any mechanism that would, by design or as a secondary effect, prohibit users from copy pasting a password in a password field, both during password creation and authentication.

Except when sent by regular mail, passwords should never be communicated in cleartext, in particular by e-mail. Only temporary or one-time passwords could be communicated in such a way.

When sending passwords by regular mail, the Commission recommends adding measures to detect any interception (e.g.: Envelopes whose interior is blackened to prevent reading by transparency, scratch boxes) or to prevent its use (e.g.: forced renewal when the password sent is used for the first time).

When sending links to create or renew a password, they should have a short expiration period, at most 24 hours, except if sent by regular mail in which case the period of validity could be longer.

When a password is refused during its creation, a clear information message reminding the organization's policy in terms of password and explaining the reason for the refusal must be displayed to the user.

The Commission considers that, as far as possible, the data controller should advise and guide the user in creating his password.

It recommends refusing any commonly used passwords. The size and content of the list of passwords to refuse should be proportionate to the risks and, where applicable, adapted to the context of use (e.g. including service-specific words). In all cases, the user should be informed that the most common passwords won't be accepted.

This recommendation concerns the processing of personal data. Thus, the Commission considers that the level of data sensitivity protected by the password cannot be considered low. In this context, and according to ANSSI recommendations regarding authentication as described in their guide "Recommandations relatives à l'authentification multifacteur et aux mots de passe", the Commission describes four sets of minimal requirements for password authentication to comply with this recommendation.

The first case relies mainly on password security; it consequently imposes significant requirements in terms of entropy, and thus size and complexity of passwords. In the following cases, additional measures ensure a similar level of security while using passwords with lower entropy.

Case n°1. - Password Only

When authentication is only based on a username and a password, the Commission considers that to comply with this recommendation, the complexity set in the password policy must ensure the equivalent of at least 80bits of entropy. The three examples below correspond to this entropy.

> Example 1: Passwords must be composed of at least 12 characters including upper-case and lower-case letters, numbers and special characters to be chosen in a list of at least 37 possible special characters.
> Example 2: Passwords must be at least 14 characters long, including upper-case and lower-case letters and numbers, with no required special characters.
> Example 3: Passphrases based on words in the French language must consist of at least 7 words.

As the robustness of this authentication is based exclusively on the intrinsic quality of the user's password, the data controller must be particularly vigilant with the quality of his user's password.

Case n°2 - Password with access restriction

When the authentication mechanism includes a system of access restriction (see examples below), the complexity to comply with this recommendation should ensure the equivalent of, at least, 50 bits of entropy.

> Example 1: the password must be at least 8 characters long and include 3 of the 4 categories of characters (upper-case and lower-case letters, numbers and special characters), special characters must be taken from a set of at least 11 characters;
> Example 2: Passphrases based on words in the French language must be at least 5 words long;
> Example 3: Passwords must be at least 15 digits long.

Thus, the authentication must involve a mechanism for restricting access to the account. This can take one or more of the following forms:

- a delay after several authentication failures which increases exponentially according to the number of attempts within a determined period; the Commission recommends to set this duration as more than 1 minute after 5 failed attempts, and to allow a maximum of 25 attempts per 24 hours; and/or
- a mechanism to limit automated and intensive submissions (e.g. implementation of "captcha"); and/or
- blocking the account after, at most, 10 consecutive failed authentications associated with an unblocking mechanism proportional to the identity theft risks on people in the considered processing.

The choice of the solution must take into account the likelihood of a denial of service attack, that would aim at rendering the accounts inaccessible, and its severity for the users.

Case n°3 - Password with additional information

When the authentication includes the provision of some additional information as well as an access restriction mechanism similar to case 2, to comply with this recommendation, the Commission considers that:

1) The complexity required for such a password must ensure, at a minimum, an entropy of 27 bits.
   Example 1: passwords must be at least 8 decimal digits;
   Example 2: passwords must be composed of, at least, 7 hexadecimal digits (i.e. decimal digits and letters from A to F, without distinction between upper and lower case).

2) The additional information must be either directly communicated by the controller or by the data subject. The Commission therefore recommends:
   a. to generate randomly this information in such a way that it ensures, at a minimum, a 23-bits total entropy for the information:
      Example 1: the information is an identifier of 7 random decimal digits;
      Example 2: the information is made up of 6 hexadecimal digits;
   b. to ensure that only the person and the data controller know this information and, thus, to renew it in any breach of its confidentiality;

c. when this information is as an account identifier, to dedicate the account to a single service and to be able to renew it when necessary (see section III.4);
d. to implement a device fingerprinting mechanism, which would combine a set of unique technical parameters of the person's terminal (IP address, address MAC, browser type, list of installed applications, etc.), to identify a trusted terminal (e.g.: non-public terminal) which the person would have previously validated and could revoke at any time.

3) An access restriction similar to case n°2 must be implemented.

This case implies the collection of additional information about the user's terminal. In a privacy by design and by default mindset, the proportionality of such collection should be checked before choosing this solution for any processing.

Case n°4 - Unlocking codes

When authentication is based on a device held by the person, the Commission considers that, to comply with this recommendation, the password policy must require a complexity ensuring the equivalent of, at least, 13 bits of entropy.

Example: the code size must be at least 4 decimal digits.

Authentication only concerns hardware devices owned by the person, namely smart cards or devices containing an electronic certificate or a pair of keys unlockable by password, or a technical mechanism providing the same security level.

After a fixed number of consecutive failed authentications, at most 3, the device must be blocked.

3. Storage methods

Regarding storage methods, the Commission considers that data controllers must never store passwords as clear text.

Any stored password used in an authentication mechanism must be transformed with a specialized non-reversible and secure cryptographic function (i.e. a renowned strong public algorithm whose software implementation is free of known vulnerability), such function should use a salt[4] and parameters relating to time and/or memory costs.

The Commission considers that the salt should be generated randomly and in principle have a minimum length of 128 bits. It must be generated for each user and can be stored in the same database.

Finally, the various elements (salt size, algorithms and parameters) must be regularly updated according to risks and technological advances.

4. Procedures for renewing the password and notification to the person

To comply with this recommendation, the following measures must be implemented.

The Commission recommends renewing systematically any compromised password.

All the above elements regarding sending passwords to the user either by regular mail or electronically also apply to its renewal.

Renewal

The Commission recommends to data controllers to give data subjects the means to change themselves, and independently, their password. All rules for password creation apply to this case.

[4] A salt is some extra data that is added to the message to be hashed (here, the password) to prevent two identical messages hashed on two different systems to correspond to the same hash value. Salts limit the case where an adversary would infer a user's password by looking into one of the many precomputed databases of "unsalted password/hash" pairs accessible on the Internet.

Periodic password renewal

The Commission does not recommend forcing periodic renewal of passwords on all its users.

However, a periodic renewal procedure remains necessary for privileged accounts (administration accounts). A relevant and reasonable periodicity must be defined according to the risks.

Renewal of the password on request of the user

If the renewal involves sending information (e.g.: URL, temporary password sent by email or phone), it must be sent via a previously validated communication channel (e.g.: email address, emergency electronic identification means). A new password should not be sent over a recently modified channel to prevent any compromise using the renewal phase. The duration of the embargo on recently modified channels must be proportionate to the risks of usurpation. User must be notified of any channel modification on every validated communication channel, including the one that has been modified, so that he can be alerted of any unasked modification.

If the renewal involves one or more additional elements (phone number, physical address, answer to a secret question, etc.), the Commission considers that:

- The system used to check whether the person requesting the renewal is the person holding the account should not use any question related to usually public information (e.g.: information accessible to many people on social networks such as parent's name, place of study, name of pets, etc.);
- These items should not be stored in the same space as the password verification item unless they are encrypted with a renowned strong public algorithm and the encryption key security is ensured;
- To prevent spoofing attempts based on the modification of these elements, the person must be immediately notified of any modification through identified communication channels.

The Commission recommends that the person have access to an interface allowing her or him to enter a new password. The session validity of this interface must not exceed 24 hours and only single-use renewal links must be provided.

Managing privacy breaches: notification and renewal

When a data breach impacting a password or some data linked to its renewal (e.g. email address) is detected, the Commission recommends to the data controller to notify data subjects without delay.

The Commission considers that any suspicion of a data breach on a user's passwords must lead data controllers to force their data subject to change their passwords at their next connection and to recommend them to change passwords of any services for which the same password is used.

When additional information is used (Case n°3), such information must also be renewed whenever its confidentiality cannot be guaranteed any more.

Finally, concerning data used during renewal, secret questions and their answers must also be renewed in any case of a confidentiality breach that would concern them.