Les règles de composition des mots de passe		
Cas	**Conditions**	**Recommandations pratiques**
Cas n°1 : Authentification uniquement avec un identifiant et un mot de passe	**La taille du mot de passe doit être au minimum** de 12 caractères.	Mettre en place un mécanisme contraignant pour empêcher la validation d'un mot de passe qui ne répondrait pas à ces exigences
ET	Le mot de passe doit comprendre **des lettres majuscules, des lettres minuscules, des chiffres et des caractères spéciaux – critères cumulatifs**.	
ET	Le responsable de traitement doit alerter l'utilisateur que la robustesse de cette authentification repose exclusivement sur la qualité intrinsèque de son mot de passe et, dans la mesure du possible, le conseiller dans la création de son mot de passe.	Information spécifique de l'utilisateur
Cas n°2 : Authentification avec un mot de passe et un mécanisme complémentaire de restriction d'accès au compte	La taille du mot de passe doit être **au minimum de 8 caractères**.	Mettre en place un mécanisme contraignant pour empêcher la validation d'un mot de passe qui ne répondrait pas à ces exigences
ET	Le mot de passe doit **comporter au minimum 3 des 4 critères ci-dessus** (majuscules, minuscules, chiffres, caractères spéciaux).	
ET	L'authentification doit faire intervenir une restriction de l'accès au compte, qui doit prendre une ou plusieurs des formes suivantes : - **une temporisation d'accès au compte après plusieurs échecs**, dont la durée augmente exponentiellement dans le temps ; la Commission recommande que cette durée soit supérieure à 1 minute après 5 tentatives échouées, et permette de réaliser au maximum 25 tentatives par 24 heures ; et/ou - **un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives** (p. ex. : « captcha ») ; et/ou - **un blocage du compte après 10 authentifications échouées consécutives au plus**.	Mettre en place un ou plusieurs des mécanismes recommandés par la Cnil
Cas n°3 : Authentification avec mot de passe et une information complémentaire	La taille du mot de passe doit être **au minimum de 5 caractères**.	Mettre en place un mécanisme contraignant pour empêcher la validation d'un mot de passe qui ne répondrait pas aux exigences
ET	L'authentification doit faire intervenir une information complémentaire, qui peut prendre l'une des formes suivantes : - **une information communiquée en propre par le responsable de traitement** ou la personne concernée. La Commission recommande que cette information ait une taille **d'au moins 7 caractères et ne soit connue que de la personne concernée et du responsable de traitement**. Si cette information correspond à l'identifiant du	Mettre en place un ou l'ensemble des mécanismes recommandés par la Cnil

	compte, il est recommandé que ce dernier soit propre au service (dédié exclusivement), fourni par le responsable de traitement, et uniquement connu de la personne concernée et du responsable de traitement ; et/ou - **tout paramètre technique ayant caractère d'unicité sur le terminal informatique utilisé par la personne concernée** (adresse IP, adresse MAC, user agent, etc.) pour lequel la personne a préalablement validé qu'il s'agissait d'un terminal de confiance (ex. : terminal non public) et qu'il peut à tout moment révoquer.	
ET	Une restriction de l'accès au compte doit être mise en œuvre. Elle peut prendre la forme d'une ou plusieurs des modalités suivantes : - **une temporisation d'accès au compte** après plusieurs échecs, dont la durée augmente exponentiellement dans le temps ; la Commission recommande que cette durée soit supérieure à 1 minute après 5 tentatives échouées, et permette de réaliser au maximum 25 tentatives par 24 heures ; et/ou ; - **un mécanisme permettant de se prémunir contre les soumissions automatisées et intensives de tentatives** (« captcha ») ; et/ou - **un blocage du compte après 5 authentifications échouées consécutives au plus**.	Mettre en place un ou plusieurs des mécanismes recommandés par la Cnil
Cas n°4 : Authentification avec mot de passe et matériel détenu par la personne	La taille du mot de passe doit être **au minimum de 4 chiffres**.	Mettre en place un mécanisme respectant l'ensemble des exigences par la Cnil
ET	**L'authentification ne peut concerner qu'un dispositif matériel détenu en propre par la personne concernée**, à savoir uniquement les cartes SIM, cartes à puce et dispositifs contenant un certificat électronique déverrouillable par mot de passe (token)	
ET	Un blocage du dispositif doit être mis en œuvre après **3 authentifications échouées consécutives au plus**.	