Charte du certificateur Ğ1

Une personne qui veut entrer dans la toile de confiance Ğ1, c'est-à-dire devenir membre Ğ1, doit obtenir cinq certifications de personnes qui sont déjà membres. Les membres peuvent aussi se certifier mutuellement. Chaque certification, accordée à un demander par un certificateur, dure deux ans. Pour rester dans la toile de confiance, il faut avoir au moins cinq certifications actives.

Tout membre de la Ğ1 souhaitant certifier un demandeur doit respecter cette charte. Deux cas se présentent :

- Certification d'une personne qui n'est pas encore membre de la Ğ1 : l'ensemble de cette charte s'applique aux cinq certificateurs du demandeur.
- Certification supplémentaire d'une personne qui est déjà membre : le certificateur prend les précautions énumérées sous le titre *Unicité du compte membre* et effectue la vérification relative au document de révocation

Dans les deux cas, le certificateur doit connaître l'identité du demandeur, être certain que celui-ci a compris les enjeux, et avoir une raisonnable certitude de l'unicité de son compte membre.

Unicité du compte membre

Pour protéger la communauté Ğ1, il faut que chaque membre ait un seul compte membre. En effet, si une personne se faisait certifier sous deux identités différentes, elle cocréerait deux DU quotidiens au lieu d'un, et aurait plus de facilité pour se créer d'autres comptes membres, puis attaquer la stabilité du réseau et la fiabilité des opérations. Pour éviter cela, ou au moins faciliter la détection d'une double identité, le certificateur prend les précautions suivantes avant d'accorder sa promesse de certification :

- Il dispose de plusieurs moyens de contacter le demandeur et de suffisamment d'éléments pour pouvoir le reconnaître dans un autre contexte.
- Il connaît la ville de résidence du demandeur, et a constaté que la carte des membres, dans cette ville, ne montre aucune identité qui pourrait correspondre au demandeur.
- Il visite les éventuels profils du demandeur sur les réseaux sociaux, compare les informations avec ce qu'il sait du demandeur, et cherche d'éventuelles connaissances communes.
- Il prend connaissance de l'identité des autres certificateurs, s'ils sont déjà connus.
- Il communique la présente charte au demandeur et s'assure qu'il l'a comprise et acceptée, puisqu'il sera lui-même amené à émettre des certifications après l'adhésion.

Premières recommandations au demandeur

Le certificateur vérifie que le demandeur a bien compris la procédure suivante.

1. Installer un client Duniter (actuellement Cesium, Silkaj ou Sakia) sur un appareil numérique.
2. Préparer deux phrases de passe selon ces recommandations de sécurité : une qui servira d'identifiant secret, l'autre de mot de passe. Savoir que le système n'a pas de procédure « mot de passe perdu ».
3. Choisir un pseudonyme ou décider d'utiliser son nom ou une partie de celui-ci.
4. Créer un compte portefeuille. Recevoir une clé publique, qui est utilisable comme un RIB (relevé d'identité bancaire) de ce compte.

5. Obtenir cinq promesses de certification, et si possible attendre que les certificateurs soient synchronisés avant de demander l'adhésion (d'abord par Cesium, puis auprès des certificateurs).

Rappel : qu'elle soit membre ou non, une personne peut créer autant de comptes portefeuilles qu'elle le souhaite pour répartir ses Ğ1 et limiter les risques liés à l'accès à la monnaie. Chaque création de compte nécessite de choisir deux phrases de passe et chaque compte est identifié par une clé publique. Au moment de l'adhésion, le demandeur choisit le compte portefeuille qu'il souhaite transformer en compte membre.

Promesse de certification

Le certificateur accorde sa promesse de certification s'il considère que les enjeux sont compris du demandeur et que les éléments dont il dispose permettent de raisonnablement garantir que le demandeur n'est pas encore membre. Avant de l'accorder,

- il vérifie que le demandeur a pris ses dispositions pour conserver ses phrases de passe, et qu'il a compris qu'il ne peut ni les modifier, ni les réclamer au système,
- il vérifie que le demandeur maîtrise son compte : par exemple il lui envoie quelques Ğ1 afin que le demandeur les lui renvoie.

Pour éviter toute erreur, le demandeur communique au certificateur la clé publique du compte portefeuille par lequel il demande l'adhésion. Le certificateur s'assure que cette clé publique correspond au demandeur, soit par les informations (photo, pseudo, texte libre) du profil associé, soit grâce au virement aller-retour décrit plus haut.

Il est bon que le demandeur mette en contact ses certificateurs, d'une part pour renforcer la certitude de l'unicité du compte membre, d'autre part pour que les certificateurs puissent se synchroniser.

Synchronisation

Le certificateur attend que le demandeur déclare avoir (au moins) cinq promesses de certification.

Si c'est possible, il se synchronise avec les autres certificateurs, c'est-à-dire qu'ils visent à réunir les conditions pour que les certifications aboutissent (on appelle cela l'alignement des planètes) :

- Aucun certificateur n'a atteint son plafond de 100 certifications,
- Pour chaque certificateur, au moins 5 jours se sont écoulés depuis qu'une certification qu'il a accordée a été validée.

Si un certificateur a émis une ou plusieurs certifications qui ne sont pas encore validées, cela crée de l'incertitude et peut compromettre l'aboutissement de la procédure. En effet, une telle certification sera validée lorsque les planètes seront alignées pour le demandeur concerné, ce qui dépend de nombreux paramètres en cascade[1].

[1] L'outil g1-monit permet de visualiser l'état des inscriptions en attente, et WotWizard indique la date d'entrée probable d'un postulant dans la toile de confiance.

De plus, la procédure peut échouer si le demandeur se trouve à plus de 5 pas[2] de 80 % des membres référents[3] (on appelle cela la règle de distance). Cependant, les certificateurs ne disposent pas d'outil pour prévoir cette situation.

Certification et ultimes recommandations

Le demandeur demande l'adhésion (dans Cesium, sous *Mon compte > Options*, choisir *Devenir membre*), de préférence une fois que les certificateurs sont synchronisés. Cette demande d'adhésion déclenche un compte à rebours de deux mois, pendant lequel les cinq certifications doivent être émises et validées.

Le certificateur s'assure que le demandeur a téléchargé le **document de révocation** de son compte (dans Cesium, sous *Mon compte > Options > Compte et sécurité*), et qu'il le conserve précieusement. Il vérifie qu'il a compris en quoi c'est utile :

- L'envoi du document de révocation à Duniter permet d'annuler l'adhésion, c'est-à-dire de retransformer le compte membre en compte portefeuille.
- En cas de perte des identifiants, le compte et ses Ğ1 sont perdus pour tout le monde. Mais la révocation permet d'arrêter la cocréation de Ğ1 de ce compte, ce qui est indispensable avant de demander une nouvelle adhésion avec un autre compte portefeuille.
- En cas de vol des identifiants, la révocation empêche le voleur de s'approprier les DU quotidiens de la victime et d'agir en son nom.

Le certificateur rappelle au demandeur que chaque certification est valable deux ans, et que pour rester membre, il devra toujours avoir au moins cinq certifications en cours de validité. Il devra aussi renouveler son adhésion une fois par an lorsqu'il y sera invité (dans Cesium, sous *Mon compte > Options*, choisir *Renouveler l'adhésion*).

[2] À l'issue de la procédure, le postulant sera à 1 pas du certificateur, à 2 pas des certificateurs de celui-ci, etc.
[3] Un membre est référent lorsqu'il a émis et reçu un nombre suffisant de certifications. Le caractère suffisant est défini dans la licence Ğ1.