Description des principales clefs actives dans le protocole xVote

Les clefs perdurant au-delà de la session de vote :

La bi-clef maîtresse KK^{dom} est stable (elle dure une législature), elle est liée ex-officio personnellement au magistrat de tutelle des institutions ou du plus haut fonctionnaire responsable des votations du domaine électoral. Elle a été certifiée par l'autorité de certification (C.A.). Elle authentifie les principales clefs de scrutin : clefs d'habilitation K_H, de vote K_V, des scrutateurs K_S, ainsi que la clef de chiffrement de l'Urne K_U^{dom}. Elle réside dans un module matériel de sécurité.

La bi-clef (racine) de l'autorité de certification (A.C.) délivre les identités numériques des citoyens (vID sur K_E) et des services, elle est stable et est utilisée indirectement dans le protocole. Elle certifie la clef institutionnelle K^{dom} (non illustrée) signant l'envoi des cartes de vote dématérialisées (par courriel). La partie privée est sécurisée dans un serveur ad hoc.
Rem. : il peut y avoir, en fait, plusieurs racines pour l'autorité de certification.

La clef de l'autorité de certification est reliée à la **bi-clef super-racine**, ultra-stable, dont la partie publique est inscrite dans le code de l'application et la privée réside dans un module de sécurité déposé dans un coffre-fort bancaire.

La bi-clef d'identité numérique personnelle du citoyen K_E, peut provenir d'un tiers habilité (eID, certificat qualifié, soit de qualité juridique optimale) et avoir la stabilité définie dans sa politique de certification. Elle peut aussi résulter d'un vote précédent, ou encore être créée lors du vote en cours; dans ces deux cas (vID), elle est certifiée par l'autorité de certification AC. Elle peut enfin avoir été renforcée par une opération d'authentification face-à-face (officialisation de la signature manuscrite, extérieure au vote). Cette identité numérique a la durée définie dans la politique de certification (P.C. de A.C.), avec un certain nombre de renouvellements possibles ou obligatoires lors de votes ultérieurs. Elle signe la carte de vote, pour endosser la demande, chiffre la bi-clef anonyme pour la celer, chiffre le paquet de sauvegarde de vote pour le protéger, et signe ou chiffre les corps des paquets de transactions.

La bi-clef d'application K_A et **d'adaptation du domaine K_I^{dom}** (non illustrée), elles sont certifiées par la C.A. et servent à signer (pour intégrité et authentification) le code exécutable de l'application de vote et le paquet du domaine de vote (interface utilisateur, etc.). Elles ne sont pas utilisées au sein du protocole, mais dans l'auto-contrôle à l'initialisation de l'application de vote. Elles ont une durée moyenne.

Les autres clefs ne durent que pour la session de vote :

La bi-clef d'habilitation K_H, certifiée par la C.A. Elle certifie la famille de clefs d'habilitation par locaux de vote KL_n ainsi que les clefs de transactions K_H^E liées aux identités KE, et aussi la clef de son propre frontal K_{HF}. Elle réside dans le Dorsal.

La bi-clef du frontal d'habilitation K_{HF} certifiée par la clef d'habilitation K_H. Elle signe ou chiffre le flux de la transaction initiale (protection TSL). Elle réside dans le Frontal.

La famille KL_n de bi-clefs d'habilitation par circonscription électorale 'n' élémentaire, pour l'estampille, toutes certifiées par K_H. La clef respective signe (valide) en aveugle l'estampille anonyme X de l'électeur. La famille réside dans le Dorsal, la bonne clef est

chargée fugacement dans le Transactionel au cours de la phase 3 (habilitation).

Les bi-clefs de transaction K_H^E elles dépendent de (l'identité) du citoyen E, et sont utilisées pour signer et (dé)chiffrer les paquets internes au cours de sa transaction d'habilitation. Elles sont générées et certifiées par K_H à l'issue de la phase 1 au cours de la création de la session virtuelle, elles sont chargées fugacement dans le Transactionel et résident dans les états de sessions virtuelles au sein du Dorsal.

La bi-clef de scrutation K_S, certifiée par la C.A. Elle certifie les clefs de transaction K_S^X, liées aux requêtes d'estampilles X, ainsi que de son propre frontal K_{SF}. Elle réside dans le Dorsal.

La bi-clef du frontal de scrutation K_{SF}, certifiée par la clef des scrutateurs K_S. Elle signe ou chiffre le flux de la transaction initiale (protection TSL). Elle réside dans le Frontal.

Les bi-clefs de transaction K_S^X elles dépendent de la requête d'estampille X, et sont utilisées pour signer les paquet interne et les reçu d'enregistrement au cours des transactions. Elles sont générées et certifiées par K_S et sont chargées fugacement dans le Transactionel depuis le Dorsal. Elles ne portent pas, dans leurs certificats, de lien avec X mais avec M(X).

La bi-clef de vote (de réception par l'urne) **K_V**, certifiée la C.A. Elle signe les récépissés de réception par l'urne des bulletins de vote.

La bi-clef de l'urne K_U^{dom}, certifiée par KK^{circ}. Elle dépend du domaine électoral. Elle sert au chiffrement des bulletins de vote. Sa partie publique est distribuée par la Scrutation, sa partie privée est scindée (doublement, en cascade) à la création et ne sera reconstituée qu'à l'ouverture de l'Urne.

La bi-clef anonyme (estampille) est notée **X**, elle est validée en aveugle par la clef de circonscription KL_n (n la circonscription électorale élémentaire) et reconnue de facto par le serveur de Scrutation lors de son enregistrement.

Les clefs partagées d'habilitation et de scrutation K_{SH}^E et K_{SS}^X, elles sont symétriques, dépendent (de l'identité) du citoyen E ou rsp. de la requête d'estampille X et sont garanties par les clefs respectives des frontaux. Elles authentifient les flux sécurisés des transactions suivantes (protection TSL-PSK).

La clef du facteur de masquage K_F^{dom} est symétrique et n'est qu'indirectement impliquée dans le protocole, mais elle est centrale dans le schéma. Elle dépend de du domaine électoral. Elle est générée et utilisée sécuritairement dans (une machine annexe de) la grappe des scrutateurs, elle n'est pas sauvegardée et est détruite (par écrasement) à l'instant de la clôture du scrutin.

La clef des mots de passe K_P (non illustrée) est symétrique et sert à générer et vérifier les mots de passe (MP) associés au numéro d'identification (NI) d'un électeur.

Note : Les clefs dont le titre est souligné sont les seules qu'il est nécessaire de présenter aux utilisateurs, les autres peuvent être considérées comme internes et de finalités techniques.

Note : Ne sont pas mentionnées les clefs des services de tiers de confiance : XKMS, O-DSS, XCMS, NRNP, etc.