**Part III - From the Acquirer to the Issuer.**

As we reached our last stop in the "journey", you might want to refer to the previous articles for more details.

**Part I - PIN Block... What and How??**

<https://www.linkedin.com/pulse/journey-pinblock-ahmed-hemdan-farghaly/>

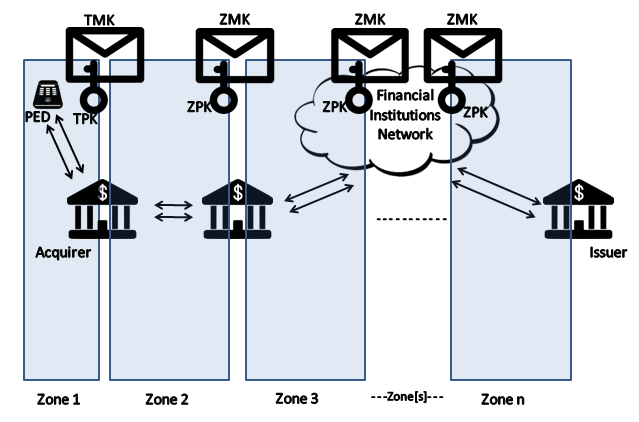
**Part II - PIN Block... first take-off and first stop.**

<https://www.linkedin.com/pulse/journey-pinblock-part-ii-ahmed-hemdan-farghaly/>

To recap, when a user enters his card PIN, a PINBlock is generated on PED [i.e. ATM/POS] {refer to part I}, then PINBlock is encrypted on PED and then transferred to acquirer along with the authorization transaction {refer to part II}.

The next an final part would be for the PINBlock to be transferred from card Acquirer to card Issuer in order to be validated.

To do this, PINBlock may travel between several payment institutions (Zones) to reach its final destination (the issuer), refer to the following illustration.



The PINBlock should be kept encrypted between all institutions till it reach the issuer this is done by the following steps.

- Between each institution and the next, there is a shared key [ZMK or Zone Master Key] which you may say the transportation means for the actual key [ZPK or Zone Pin Key].

* ZPK is the key responsible for encrypting PINBlock between zones [institutions].

- Staring with the acquirer, it will make a key exchange with the next institution (maybe a national switch or another payment processor), which will reply with a key [ZPK] encrypted under [ZMK].

- As the acquirer already have the next institution's ZMK injected in its HSM (this is a whole different process), acquirer will be able to extract the clear ZPK.

- Acquirer will then translate the PINBlock to be encrypted under the ZPK of the next institution.

- The next institution will be able to translate PINBlock using the previously shared ZPK, hence get the Clear PINBlock.

- This institution will do the same previous steps with the next institution to encrypt and transfer the PINBlock using the next institution's ZPK.

- The final stop will be at card issuer side, where it will receive the PINBlock encrypted under it's ZPK and using it's HSM, it will be able to validate if the PIN is correct or not.

**As this journey ends here, our series of articles about FinTech technologies will continue, hoping to understand more, learn more from each other along the journey.**

See you in another exciting FinTech Subject...