# Detalizētais audita aktivitāšu apraksts

1. Pārbaudīt vai tiek ievērota drošības politika pret atslēgu glabāšanu un izmantošanu:

* Konstatēt, ka atslēgas tiek glabātas HSM (hardware secure module) iekārtā iekš atsevišķi izdalīta slotā (aparatūras atmiņas segments);
* Pārbaudīt lietotāju autorizācijas drošības vadlīnijas - vismaz diviem lietotājiem ir jābūt autorizētiem, lai veiktu nepieciešamas operācijas ar atslēgām slota ietvaros;
* Pārliecināties, ka atslēgu importēšanas un eksportēšanas privilēģijas ir piešķirtas tikai drošības vadītāju (security officer) lietotāju kontiem, t.i., parastiem lietotājiem nav dotas šīs iespējas;
* Pārbaudīt LMK un ZMK atslēgu glabāšanas drošības vadlīnijas. ZMK ir primāra atslēga zem kuras tiek importētas jaunas atslēgas, bet LMK ir atslēga tiek lietota no HSM eksportēto atslēgu šifrēšanai. Secīgi ir jāpārbauda vai doto atslēgu komponentes ir sadalītas starp atbilstošiem lietotājiem, tas tiek glabātas katrām lietotājam atbilstoša seifā;
* Veikt pierakstu žurnāla ekspertizi, sameklējot ierakstus par atslēgu importēšanas ceremonijām. Pārliecināties, ka dotie lietotāji ir iesaistījušies dota procedūrā un ir pilntiesīgi glabāt doto atslēgu komponentes.
* Pieprasīt apsardzei video ierakstus, kuros ir uzņemta atslēgu importēšanas ceremonijā.

1. Pārbaudīt vai tiek ievēroti drošības pasākumi pret ienākošiem datiem:

* Konstatēt, ka ienākošas datnes no bankām tiek šifrētas ar PGP algoritma palīdzību;
* Konstatēt, ka programmatūra prot apstrādāt šifrētas datnes;
* Pārbaudīt, ka failu atšifrēšanai izmantota PGP atslēga tiek glabāta iekš HSM - programmatūra, balstoties uz iestatījumiem, datu apstrādes laikā spēj pieslēgties atbilstošam HSM slotām.

1. Pārbaudīt vai tiek pildīti MasterCard un Visa noteikumi apstrādāto datu un PIN aplokšņu vadībai:

* Pieprasīt apsardzei video ierakstus ar mērķi pārliecināties, ka sabojātas PIN aploksnes tiek iznīcinātas uz vietas;
* Pieprasīt žurnālu, kurā ir reģistrētas pēdējo apstrādāto datņu un izdrukāto PIN aplokšņu partijas. Pretī katrai partijai ir jābūt banku kurjeru parakstiem;
* Pārbaudīt, ka apstrādātas datnes pēc noteikta laika tiek izdzēstās no failu sistēmas. Pa šo laiku datnei ir jānonāk personalizācijas telpā. Failu dzēšanai jābūt automatizētai, kas tiek veikta ar speciāla skripta, robota palīdzību.

1. Pārbaudīt vai ir paredzētas atslēgu rezerves kopijas un ir noteiktas iespējas to atjaunošanai vadoties pēc drošības normatīviem:

* Pārliecināties vai ir izveidota atslēgu rezerves kopija;
* Pārliecināties vai ir izveidota atjaunošanas, backup, atslēga, kas ļaus importēt atslēgu rezerves kopiju arhīvu;
* Noteikt vai atjaunošanas atslēgas komponentes ir sadalītas starp lietotājiem un tiek glabātas droša vieta. Veicot lietotāju aptauju, pārbaudot video ierakstus un apmeklētāju žurnālu.