[0301] As shown by reference number 1520 in FIG. 15, POS partner/terminal 1504 generates a session key (DUKPT) (e.g., a session secret key ss_k, etc.) using the DUKPT method (e.g., DUKPT = KDF(MSK, Nonce), where KDF is a key derivation function and MSK is a Master Session Key, etc.)

[0302] As shown by reference number 1522 in FIG. 15, POS partner/terminal 1504 encrypts an authentication code (e.g., a PIN, etc.) for a transaction using the triple-DES algorithm TDES and the session key (DUKPT) to generate a PIN block (EPB) (e.g., EPB = TDES(PIN, DUKPT), etc.)

[0303] As shown by reference number 1524 in FIG. 15, POS partner/terminal 1504 encrypts the session key (DUKPT) based on the POS partner public key (pk_{pos}) using the function PRE.E(DUKPT, pk_{pos}) (e.g., wraps the session secret key ss_k with the POS partner public key (pk_{pos}) to generate DUKPT'). For example, POS partner/terminal 1504 generates encrypted transaction data (e.g., authorization request cryptogram (ARQC), EPB, DUKPT') for a transaction, the encrypted transaction data comprising: (i) an encrypted code (EPB) comprising an authentication code (PIN) encrypted with a session key (DUKPT), and (ii) an encrypted session key (DUKPT') comprising the session key (DUKPT) encrypted with the POS partner public key (pk_{pos}) associated with POS partner/terminal 1504.

[0304] As shown by reference number 1526 in FIG. 15, POS partner/terminal 1504 communicates the encrypted transaction data (e.g., ARQC, EPB, DUKPT') to payment gateway 1506. For example, payment gateway 1506 receives, from POS partner/terminal 1504, the encrypted transaction data (ARQC, EPB, DUKPT') for the transaction, the encrypted transaction data comprising: (i) the encrypted code (EPB) comprising the authentication code (PIN) encrypted with the session key (DUKPT), and (ii) the encrypted session key (DUKPT') comprising the session key (DUKPT) encrypted with the POS partner public key (pk_{pos}) associated with POS partner/terminal 1504.

[0305] As shown by reference number 1528 in FIG. 15, payment gateway 1506 determines a re-encryption key ($rk_{pos->mb}$) from the re-encryption keys ($rk_{pos->mb}^1$, …, $rk_{pos->mb}^n$) based on the encrypted transaction data. For example, payment gateway 1506 determines the re-encryption key ($rk_{pos->mb}$) from the re-encryption keys ($rk_{pos->mb}^1$, …, $rk_{pos->mb}^n$) that corresponds with a merchant bank public key (pk_{mb}) of the merchant bank public keys (pk_{mb}^1, …, pk_{mb}^n).

[0306] As shown by reference number 1530 in FIG. 15, payment gateway 1506 re-encrypts the encrypted session key (DUKPT') with the re-encryption key ($rk_{pos->mb}$) using the re-encryption function PRE.RE (e.g., DUKPT'' = PRE.RE(DUKPT', $rk_{pos->mb}$)) to generate a re-encrypted encrypted session key DUKPT''.

[0307] As shown by reference number 1532 in FIG. 15, payment gateway 1506 communicates the re-encrypted encrypted session key (DUKPT'') to merchant bank 1508. For example, merchant bank 1508 may receive, from payment gateway 1506, the encrypted transaction data (e.g., ARQC, EPB, DUKPT'') comprising: (i) an encrypted code (EPB) comprising an authentication code (PIN) encrypted with a session key (DUKPT), and (ii) a re-encrypted encrypted session key (DUKPT'') comprising an encrypted session key (DUKPT') encrypted with the re-encryption key ($rk_{pos->mb}$), the encrypted session key (DUKPT') comprising the session key (DUKPT) encrypted with the POS partner public key (pk_{pos}) associated with POS partner/terminal 1504.

[0308] As shown by reference number 1534 in FIG. 15, merchant bank 1508 may decrypt the re-encrypted encrypted session key (DUKPT'') based on the merchant bank secret key (sk_{mb}) using the function PRE.D. In some non-limiting embodiments or aspects, merchant bank 1508 generates an authorization request message in response to verifying the authentication code (PIN) and communicates the authorization request message to payment network 1510.

[0309] As shown by reference number 1536 in FIG. 15, merchant bank 1508 may generate and forward, to payment network 1510, encrypted transaction data (e.g., ARQC, EPB, DUKPT') for the transaction, the encrypted transaction data comprising: (i) an encrypted code (EPB) comprising an authentication code (PIN) encrypted with a session key (DUKPT), and (ii) an encrypted session key (DUKPT') comprising the session key (DUKPT) encrypted with the merchant bank public key (pk_{mb}) associated with merchant bank 1508. For example, payment network 1510 may receive the encrypted transaction data (e.g., ARQC, EPB, DUKPT') for the transaction, the encrypted transaction data comprising: (i) the+ encrypted code (EPB) comprising the authentication code (PIN) encrypted with the session key (DUKPT), and (ii) an encrypted session key (DUKPT') comprising the session key (DUKPT) encrypted with the merchant bank public key (pk_{mb}) associated with merchant bank 1508.

[0310] As shown by reference number 1538 in FIG. 15, payment network 1510 may determine a re-encryption key ($rk_{mb->cb}$) from the re-encryption keys ($rk_{mb->cb}^{1}$, …, rk_{mb-}

$_{>cb}^{n}$) based on the encrypted transaction data. For example, payment network 1510 determines the re-encryption key ($rk_{mb->cb}$) from the re-encryption keys ($rk_{mb->cb}^{1}$, …, $rk_{mb->cb}^{n}$) that corresponds with a consumer bank public key (pk_{cb}) of the consumer bank public keys (pk_{cb}^{1}, …, pk_{cb}^{n}).

[0311] As shown by reference number 1540 in FIG. 15, payment network 1510 re-encrypts the encrypted session key (DUKPT') with the re-encryption key ($rk_{mb->cb}$) using the re-encryption function PRE.RE (e.g., DUKPT'' = PRE.RE(DUKPT', $rk_{mb->cb}$)).

[0312] As shown by reference number 1542 in FIG. 15, payment network 1510 communicates the re-encrypted encrypted session key (DUKPT'') to consumer bank 1512. For example, consumer bank 1512 may receive, from payment network 1510, the encrypted transaction data (e.g., ARQC, EPB, DUKPT'') comprising: (i) an encrypted code (EPB) comprising an authentication code (PIN) encrypted with a session key (DUKPT), and (ii) a re-encrypted encrypted session key (DUKPT'') comprising an encrypted session key (DUKPT') encrypted with the re-encryption key ($rk_{mb->cb}$), the encrypted session key (DUKPT') comprising the session key (DUKPT) encrypted with the merchant bank public key (e.g., pk_{mb}) associated with merchant bank 1508.

[0313] As shown by reference number 1544 in FIG. 15, consumer bank 1512 may decrypt the re-encrypted encrypted session key (DUKPT'') based on the consumer bank secret key (sk_{cb}) using the function PRE.D (e.g., DUKPT = PRE.D(DUKPT'', sk_{cb})) to get the session key (DUKPT) and decrypt the encrypted code (EPB) using the session key (DUKPT) (e.g., PIN = TDES(DUKPT, EPB), etc.) to get the authentication code (PIN).

[0314] As shown by reference number 1546 in FIG. 15, consumer bank 1512 may authorize (or deny) the transaction based on the authentication code (PIN).

[0315] Example Offline Consumer Bank

[0316] Referring now to FIG. 16, FIG. 16 is a diagram of an overview of a non-limiting embodiment or aspect of an implementation 1600 relating to a process for securely transmitting PINs and other sensitive data. As shown in FIG. 16, implementation 1600 includes payment network 1610, consumer bank 1612, and trusted hardware 1614. In some non-limiting embodiments or aspects, payment network 1610 can be the same or similar to payment network 310. In some non-limiting embodiments or aspects, consumer bank 1612 can be the same or similar to consumer bank 312.

[0317] As shown by reference number 1620 in FIG. 16, consumer bank 1612 may authorize payment network 1610 to provision the consumer bank secret key (sk_{cb}) to trusted hardware 1614 (e.g., Intel SGX hosted extended access point, etc.).

[0318] As shown by reference number 1622 in FIG. 16, payment network 1610 re-encrypts the encrypted session key (DUKPT') for a transaction with the re-encryption key ($rk_{mb->cb}$) using the re-encryption function PRE.RE (e.g., DUKPT'' = PRE.RE(DUKPT', $rk_{mb->cb}$)).

[0319] As shown by reference number 1624 in FIG. 16, payment network 1610 attempts to send the encrypted transaction data for the transaction to consumer bank 1612 and detects that consumer bank 1612 is offline.

[0320] As shown by reference number 1626 in FIG. 16, payment network 1610 requests trusted hardware 1614 for authorization of the transaction. For example, payment network 1610, in response to determining that the consumer bank 1612 is offline, requests trusted hardware 1614 for authorization of the transaction by providing the encrypted transaction data (e.g., ARQC, EPB, DUKPT'') to trusted hardware 1614.

[0321] As shown by reference number 1628 in FIG. 16, trusted hardware 1614 may decrypt the re-encrypted encrypted session key (DUKPT'') based on the consumer bank secret key (sk_{cb}) using the function PRE.D (e.g., DUKPT = PRE.D(DUKPT'', sk_{cb})) to get the session key (DUKPT) and decrypt the encrypted code (EPB) using the session key (DUKPT) (e.g., PIN = TDES(DUKPT, EPB), etc.) to get the authentication code (PIN).

[0322] As shown by reference number 1630 in FIG. 16, trusted hardware 1614 may authorize (or deny) the transaction based on the authentication code (PIN).

[0323] Example Key Setup

[0324] Referring now to FIG. 17, FIG. 17 is a diagram of an overview of a non-limiting embodiment or aspect of an implementation 1700 relating to a process for securely transmitting PINs and other sensitive data. As shown in FIG. 17, implementation 1700 includes POS partner/terminal 1704, payment gateway 1706, merchant bank 1708, payment network 1710, and consumer bank 1712. In some non-limiting embodiments or aspects, POS partner/terminal 1704 can be the same or similar to POS partner/terminal 304. In some non-limiting embodiments or aspects, payment gateway 1706 can be the same or similar to payment gateway 306. In some non-limiting embodiments or aspects, merchant bank 1708 can be the same or similar