ΤΡΑΠΕΖΑ ΤΗΣ ΕΛΛΑΔΟΣ
Δ/ΝΣΗ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΜΗΜΑ ΥΠΟΣΤΗΡ.ΕΞΟΠΛ.& ΛΕΙΤ.ΣΥΣΤΗΜΑΤΩΝ

ΣΥΝΟΠΤΙΚΕΣ ΤΕΧΝΙΚΕΣ ΟΔΗΓΙΕΣ

ΓΙΑ ΤΗΝ ΣΥΝΔΕΣΗ

ΣΤΗΝ ΠΛΑΤΦΟΡΜΑ SSP/TARGET2 (ICM)

Σαράντης Σακαρίδης

Αθήνα, Ιούλιος 2007

ΠΕΡΙΕΧΟΜΕΝΑ Σελ.

ΕΙΣΑΓΩΓΗ

Οπως είναι ήδη γνωστό, το τραπεζικό σύστημα της Ελλάδας θα ενταχθεί σύντομα (Μάιος 2008) στο περιβάλλον του Target2, γνωστού και ως SSP (Single Shared Platform), το οποίο αποτελεί την μετεξέλιξη του υφισταμένου συστήματος Target.

Η Τράπεζα της Ελλάδος, στα πλαίσια του συντονιστικού και καθοδηγητικού της ρόλου στο ως άνω έργο, οργανώνει σειρά ενημερωτικών συναντήσεων και σεμιναρίων, προκειμένου να υποστηρίξει με τον καλύτερο δυνατό τρόπο την Ελληνική Τραπεζική Κοινότητα στην μετάβασή της στο νέο αυτό περιβάλλον.

Το συγκεκριμένο σεμινάριο έχει σκοπό την ενημέρωση των Τραπεζών σχετικά με την διενέργεια των απαραίτητων δοκιμών χρηστών (User Tests). Για το θέμα αυτό είναι ήδη διαθέσιμο και έχει διανεμηθεί σχετικό υλικό τεκμηρίωσης. Δεδομένου δε ότι το Target2 χρησιμοποιεί ως φορέα/υποδομή το ήδη υφιστάμενο διατραπεζικό Δίκτυο SWIFTNet, είναι επίσης διαθέσιμη και όλη η σχετική τεκμηρίωση των προϊόντων του SWIFTNet (Version 6.0). Το υλικό τεκμηρίωσης προέρχεται, κατά συνέπεια, από δύο πηγές (Target2, SWIFT) και είναι εξαιρετικά εκτεταμένο.

Με βάση τα παραπάνω και με σκοπό να διευκολυνθούν οι Τράπεζες στην προετοιμασία του τεχνικού τους περιβάλλοντος και στην διαμόρφωση των απαραίτητων προϋποθέσεων για την επιτυχή εκτέλεση των δοκιμών, έχει εκπονηθεί το παρόν εγχειρίδιο. Πρόκειται για μια σύνοψη των σχετικών πληροφοριών σε τεχνικό επίπεδο, με συγκεκριμένο πρακτικό προσανατολισμό. Είναι αυτονόητο ότι η επίσημη τεκμηρίωση, τόσο του Target2 όσο και του SWIFT, θεωρείται ούτως ή άλλως απαραίτητη.

ΣΥΝΤΟΜΗ ΑΝΑΦΟΡΑ ΣΤΙΣ ΥΠΗΡΕΣΙΕΣ SWIFTNet ΤΟΥ TARGET2

Το σύστημα Target2 χρησιμοποιεί το διατραπεζικό δίκτυο SWIFT/SWIFTNet και αξιοποιεί με κατάλληλο τρόπο τις υπηρεσίες που αυτό προσφέρει. Συγκεκριμένα ισχύουν τα εξής:

SWIFTNet FIN και SWIFTNet FINCopy

Ενα μέλος του Target2 χρησιμοποιεί FIN μηνύματα MT103, MT103+, MT202 και MT204 για τη διακίνηση εντολών πληρωμής. Επίσης μπορούν να χρησιμοποιηθούν μεταξύ των αμέσων μελών και ορισμένοι ακόμη τύποι μηνυμάτων (π.χ. MT999, 191, 192, 199 κλπ) για σκοπούς πληροφόρησης και ελέγχου.
Ο μηχανισμός FINCopy χρησιμοποιείται για να προωθήσει μια εντολή πληρωμής προς το υποσύστημα πληρωμών (Payments Module – PM) του Target2. Το Target2 λαμβάνει ένα πλήρες αντίγραφο του σχετικού FIN μηνύματος και μπορεί εν συνεχεία να επιτρέψει ή να εμποδίσει την παράδοση του μηνύπατος στον παραλήπτη. Το SWIFT αποθηκεύει το FIN μήνυμα μέχρι την οριστική "έγκριση" ή απορριψή του από το Target2.
Για την εξυπηρέτηση των παραπάνω λειτουργιών έχει δημιουργηθεί μια κλειστή ομάδα χρηστών FIN (Closed User Group – CUG) με τον κωδικό TGT, η οποία στα πλαίσια της SSP είναι γνωστή ως "FIN Y-Copy PM".

SWIFTNet InterAct (IA)

Η υπηρεσία αυτή παρέχει τη δυνατότητα ανταλλαγής σε πραγματικό χρόνο (real-time) πληροφοριών και οδηγιών μεταξύ του Target2 και των αμέσων μελών του. Για παράδειγμα τα μέλη μπορούν να παρακολουθούν στοιχεία σχετικά με πιστωτικούς κινδύνος ή να διαχειρίζονται τη ρευστότητά τους.

SWIFTNet FileAct (FA)

Μέσω της υπηρεσίας αυτής είναι δυνατή η ανταλλαγή μεγάλων όγκων δεδομένων. Το Target2 χρησιμοποιεί το FileAct για την αποστολή αναφορών (reports) και για τη διανομή του Target2 Directory. Πιο αναλυτικά, το Target2 κάνει χρήση της υπηρεσίας αυτής με δύο τρόπους, ως εξής:

- Real-time File-download mode / Pull mode, όπου τα μέλη του Target2 ζητούν και λαμβάνουν πληροφορίες με δική τους πρωτοβουλία (initiation), π.χ. για να παραλάβουν το Target2 Directory ή ογκώδεις αναφορές (reports).
- Store-and Forward (SnF) mode, όπου το Target2 αποστέλλει, με δική του πρωτοβουλία, πληροφορίες με μορφή αρχείου (file) στα μέλη, όπως π.χ. τις ενημερώσεις του Target2 Directory.

SWIFTNet Browse

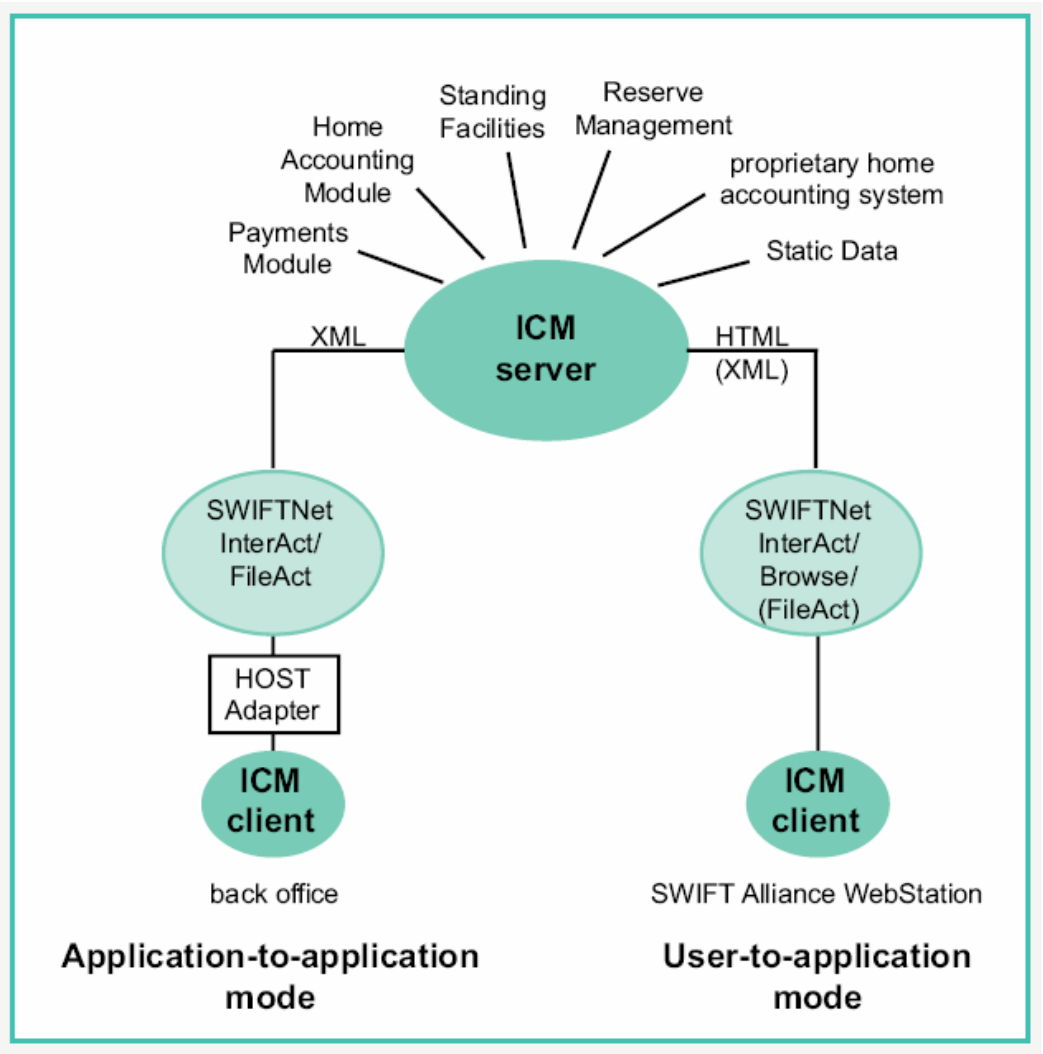
Το SWIFTNet Browse επιτρέπει την ασφαλή πρόσβαση στους Web-Servers που λειτουργούν στο περιβάλλον του SWIFTNet / SIPN, με χρήση ενός προγράμματος πλοήγησης στο Internet (Web-Browser). Στα πλαίσια του Target2 η υπηρεσία αυτή επιτρέπει στα μέλη να "βλέπουν" ένα πλήθος πληροφοριών, όπως π.χ. η ουρά εντολών πληρωμής, η κατάσταση (status) του συστήματος κλπ. Επίσης μέσω του λογισμικού WebStation (SAB) είναι δυνατόν να συνδυαστεί η διακίνηση μηνυμάτων τύπου InteAct και FileAct.

PAPSS – Payment and Accounting Processing Services

Οι παραπάνω αναφερθείσες υπηρεσίες αποτελούν κατά βάση θεμελιώδη συστατικά στοιχεία του περιβάλλοντος του SWIFTNet (Core SWIFTNet messaging Services). Η συνδυασμένη χρήση τους με βάση συγκεκριμένες προδιαγραφές και για την εξυπηρέτηση ειδικού σκοπού επιτρέπει την ανάπτυξη νέων υπηρεσιών, που απευθύνονται σε ειδικό κοινό (Closed User Groups – CUGs) και καλύπτουν συγκεκριμένες ανάγκες.
Στα πλαίσια του Target2 έχει αναπτυχθεί η υπηρεσία PAPSS (Payment and Accounting Processing Services), μέσω της οποίας παρέχεται πρόσβαση στο υποσύστημα ICM. Ακολουθώντας τους σχετικούς κανόνες του SWIFTNet έχουν ορισθεί δύο διαφορετικές υπηρεσίες, μια για κάθε ένα από τα περιβάλλοντα δοκιμών (Test/Pilot) και παραγωγής (Live). Δεδομένου και του διαχωρισμού μεταξύ Real-time και Store-and-Forward mode, προκύπτει ο παρακάτω πίνακας, στον οποίο φαίνονται οι διάφορες μορφές της υπηρεσίας PAPSS:

	PAPSS Live service name	PAPSS Pilot service name
Real-time	trgt.papss	**trgt.papss!p**
Store-and-Forward	trgt.sfpapss	**trgt.sfpapss!p**

ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΤΟΥ ICM



Από το πιο πάνω σχήμα φαίνεται ότι η πρόσβαση στο υποσύστημα ICM του Target2 είναι δυνατόν να επιτευχθεί με δύο τρόπους:

- Application-to-Application (**A2A**)
- User-to-Application (**U2A**)

Στην πρώτη περίπτωση (A2A) οι πληροφορίες και τα μηνύματα XML διακινούνται απ'ευθείας μεταξύ της SSP και της εσωτερικής εφαρμογής της συμμετέχουσας Τράπεζας-μέλους. Η εφαρμογή αυτή μπορεί να έχει αναπτυχθεί in-house ή να έχει αγορασθεί ως έτοιμη λύση. Η μέθοδος αυτή επιτρέπει την ανάπτυξη ποικίλων αυτοματισμών.

Η δεύτερη μέθοδος (U2A) παρέχει στους χρήστες της συμμετέχουσας Τράπεζας-μέλους τη δυνατότητα άμεσης επικοινωνίας με το υποσύστημα ICM. Οι πληροφορίες εμφανίζονται στην οθόνη του υπολογιστή του χρήστη (PC) με τη βοήθεια ενός προγραμματος πλοήγησης στο Internet (Web Browser), ενώ το PC πρέπει να είναι εφοδιασμένο με ειδικό έτοιμο λογισμικό (Swift Alliance weBstation – SAB). Κατά συνέπεια δεν απαιτείται η ανάπτυξη ειδικής εφαρμογής.

ΑΠΑΙΤΟΥΜΕΝΟ ΛΟΓΙΣΜΙΚΟ SWIFT ΓΙΑ ΠΡΟΣΒΑΣΗ ΣΤΟ ICM

Η πρόσβαση στο ICM του Target2 (με τη μορφή U2A – User-To-Application) είναι εφικτή μόνο με τη χρήση του λογισμικού SWIFT Alliance WebStation (SAB). Οι δυνατοί τρόποι σύνδεσης είναι:

- Μεμονομένο SAB (standalone)
- SAB που συνδέεται στο SIPN μέσω SAG (SWIFT Alliance Gateway)
- SAS (SWIFT Alliance StarterSet)

Στην περίπτωση σύνδεσης μέσω SAG είναι σημαντικό να εξασφαλιστεί ότι η ισχύουσα άδεια χρήσης SAG καλύπτει το επιθυμητό πλήθος των ταυτόχρονα συνδεδεμένων χρηστών.

Το λογισμικό SAB πρέπει να εγκατασταθεί στα PCs που θα συνδεθούν στο ICM. Σχετικές αναλυτικές οδηγίες υπάρχουν στο SWIFTNet-document: “SAB 6.0 – Installation Guide”.

Οταν το SAB συνδέεται στο SIPN μέσω SAG, είναι απαραίτητο να διαμορφωθεί ένας **Proxy Server** στο περιβάλλον του SAG. Αυτός συνήθως υλοποιείται με τη βοήθεια του λογισμικού Apache (το οποίο θα πρέπει να εγκατασταθεί, αν δεν υπάρχει ήδη) και με χρήση συγκεκριμένων ρυθμίσεων. Σχετικές οδηγίες υπάρχουν στο SWIFTNet-document: “SAG 6.0 Operations Guide – Chapter 12”.

Επιπλέον των ανωτέρω, είναι απαραίτητο να παραμετροποιηθεί με κατάλληλο τρόπο το αντίστοιχο **Firewall**, προκειμένου να επιτρέπει τη διακίνηση πακέτων που αφορούν την υπηρεσία **Browse** (SWIFTNet Browse Service). Στα επόμενα παρατίθενται συγκεκριμένες πληροφορίες για το ζήτημα αυτό.

ΔΙΕΥΘΥΝΣΕΙΣ (URLs) ΓΙΑ ΤΗΝ ΣΥΝΔΕΣΗ ΜΕ ΤΟ ICM

Η σύνδεση με το ICM μέσω του δικτύου SIPN του SWIFT επιτυγχάνεται με χρήση των εξής διευθύνσεων (URLs):

- Test ICM: https://trgt-papss-cust.ssp.swiftnet.sipn.swift.com
- Live ICM: https://trgt-papss.ssp.swiftnet.sipn.swift.com

ΔΙΑΜΟΡΦΩΣΗ ΤΟΥ SAB-PC ΓΙΑ ΧΡΗΣΗ ΤΟΥ ICM

Αυτή επιτυγχάνεται εφαρμόζοντας τα υποδεικνυόμενα βήματα, όπως αυτά περιγράφονται στο SWIFTNet-document: “SAB 6.0 User Guide – Chapter 2.1”. Συνοπτικά θα πρέπει να γίνουν τα εξής:

Εγγραφή-δημιουργία ενός (τουλάχιστον) SWIFTNet χρήστη (SN-user), ο οποίος θα χρησιμοποιήσει την υπηρεσία SWIFTNet Browse και εκδοση του σχετικού πιστοποιητικού (SN-user Certificate). Στον υπ’ όψη SN-user εκχωρείται σχετικό password (passwd-1). Αρμόδιος για το βήμα αυτό είναι ο υπεύθυνος ασφαλείας του οργανισμού-εταιρείας για το SWIFTNet (SWIFTNet Security Officer – SO).

Διαμόρφωση-παραμετροποίηση του Internet Explorer (IE):

- Ορισμός του κατάλληλου HTTP Proxy Server. Αυτός είναι συνήθως ο Proxy που βρίσκεται στο περιβάλλον SAG.

- Καθορισμός των παραμέτρων ασφαλείας (security settings) – SAB 6.0 User Guide.

- Απόκτηση και ενσωμάτωση στο περιβάλλον του IE του πιστοποιητικού Αρχής Πιστοποίησης (CA Certificate) του SWIFT (URL: http://wbcl01.swiftnet.sipn.swift.com/cacert.der)

- Πιστοποίηση του Browser (δηλ. του IE): Το βήμα αυτό εκτελείται σε δύο στάδια. Σε πρώτη φάση, ο SWIFTNet Security Officer δημιουργεί ένα πιστοποιητικό (Browser Certificate) για το συγκεκριμένο SAB-PC και το οποίο συνοδεύεται από ειδικούς κωδικούς ενεργοποίησης (μιας χρήσης). Σε δεύτερη φάση γίνεται ενεργοποίηση του ως άνω πιστοποιητικού από τον χρήστη του SAB-PC, με τη βοήθεια ενός System (ή Network) administrator. Το πιστοποιητικό αυτό εφοδιάζεται με ειδικό password (passwd-2). Είναι σημαντικό, το ως άνω πιστοποιητικό να χαρακτηρισθεί με *Security Level:* **High**.

- Ενσωμάτωση στον IE των συνδέσμων (links) που θα χρησιμοποιηθούν για την πρόσβαση στο ICM. Οι σύνδεσμοι αυτοί έχουν ήδη αναφερθεί παραπάνω (Test ICM, Live ICM).

- Προκειμένου να εξασφαλισθεί η ορθή λειτουργία των χειρισμών-buttons: “Save” και “Print” στις διάφορες οθόνες του ICM, θα πρέπει οι ακόλουθες διευθύνσεις (URLs) να εισαχθούν επιπλέον και στη λίστα των “trusted sites” του IE:

  https://trgt-papss-cust.ssp.swiftnet.sipn.swift.com (Test ICM)
  https://trgt-papss.ssp.swiftnet.sipn.swift.com (Live ICM)

- Τέλος για τη βελτιστοποίηση της λειτουργίας της εφαρμογής του ICM, προτείνεται να ορισθεί το μέγεθος της Cache του Browser (IE) από 1,5 MB έως 2 MB.

ΡΥΘΜΙΣΕΙΣ ΣΤΟ FIREWALL ΓΙΑ ΤΟ SWIFTNet Browse Service - ICM

Οι συνιστώμενες από το SWIFT ρυθμίσεις στο Firewall για την λειτουργία της υπηρεσίας SWIFTNet Browse (όπως αυτές περιγράφονται στο SWIFTNet-document: “Network Configuration Tables Guide”) έχουν συνοπτικά την εξής μορφή:

- Για όλες τις IP διευθύνσεις στο διάστημα 149.134.0.0 /17 (ή αλλιώς: 149.134.0.0 / netmask 255.255.128.0) θα πρέπει να υπάρχουν κανόνες (firewall rules) που να επιτρέπουν την εξερχόμενη κυκλοφορία TCP (outgoing TCP sessions), από τα SAB-PCs προς τις παραπάνω διευθύνσεις και εδικότερα προς το TCP-port: 443 (HTTPS).

- Εναλλακτικά, σε περίπτωση χρήσης SAG, οι αντίστοιχοι κανόνες θα πρέπει να επιτρέπουν εξερχόμενη TCP κυκλοφορία από τον SAG Server προς τις ως άνω διευθύνσεις, TCP-port: 443, ενώ παράλληλα το Firewall θα πρέπει να επιτρέπει τη σύνδεση των SAB-PCs στον Proxy Server του SAG, στο αντίστοιχο TCP-port (π.χ. 8080).

- Το παραπάνω εύρος IP διευθύνσεων καλύπτει όλες περιπτώσεις υπηρεσιών SWIFTNet Browse, είτε αυτές παρέχονται από το ίδιο το SWIFT, είτε από

άλλους Service Providers (π.χ. SSP/Target2-ICM), πάντα όμως μέσω του SIPN.

Εάν οι ως άνω συστάσεις δεν είναι αποδεκτές από τον οργανισμό-εταιρεία για λόγους εσωτερικής πολιτικής ασφαλείας, μπορεί να χρησιμοποιηθεί εναλλακτικά ο ακόλουθος πίνακας διευθύνσεων IP, προκειμένου να επιτραπεί η πρόσβαση μέσω SAB/ICM στο περιβάλλον δοκιμών του Target2:

URL	A	B	C	D
trgt-papss-cust.ssp.swiftnet.sipn.swift.com	149.134.0.101	149.134.0.152	149.134.0.125	149.134.0.134

Εννοείται ότι στην περίπτωση αυτή θα πρέπει να επιτρέπεται η εξερχόμενη κυκλοφορία προς τις ως άνω συγκεκριμένες IP διευθύνσεις.

ΧΡΗΣΙΜΕΣ ΥΠΟΔΕΙΞΕΙΣ ΓΙΑ ΤΗ ΧΡΗΣΗ ΤΟΥ SAB-PC / ICM

Με δεδομένο ότι έχουν ολοκληρωθεί με επιτυχία οι απαραίτητες ρυθμίσεις, όπως αυτές έχουν περιγραφεί στα προηγηθέντα, τα βασικά βήματα για την σύνδεση με το ICM (μέσω του SAB-PC και του SIPN) είναι τα παρακάτω:

1. Εκκίνηση του λογισμικού WebStation (SAB), με διπλό click στο σχετικό εικονίδιο.

2. Πληκτρολόγηση του User Name του SN-user και του σχετικού password (passwd-1). Το Logon mode είναι: SWIFTNet User).

3. (Προαιρετικά:) Ελεγχος σύνδεσης με SWIFTNet: Group (Selector Button): “Admin” στην αριστερή πλευρά, εικονίδιο “Check Link” και, εν συνεχεία, “Send test message” button. Η ενέργεια αυτή κάνει χρήση της υπηρεσίας “swift.cte” του SWIFT και το επιτυχές αποτέλεσμα εξασφαλίζει ότι υπάρχει σύνδεση με το περιβάλλον του SWIFTNet.

4. Ενεργοποίηση του Browsing Mode: Group (Selector Button): “Browsing” στην αριστερή πλευρά, εικονίδιο: “Control”, “Start” button. Αυτόματα ανοίγει ένα δεύτερο (θυγατρικό) παράθυρο, το οποίο στην φέρει την ένδειξη “IAB Started” στην γραμμή τίτλου.

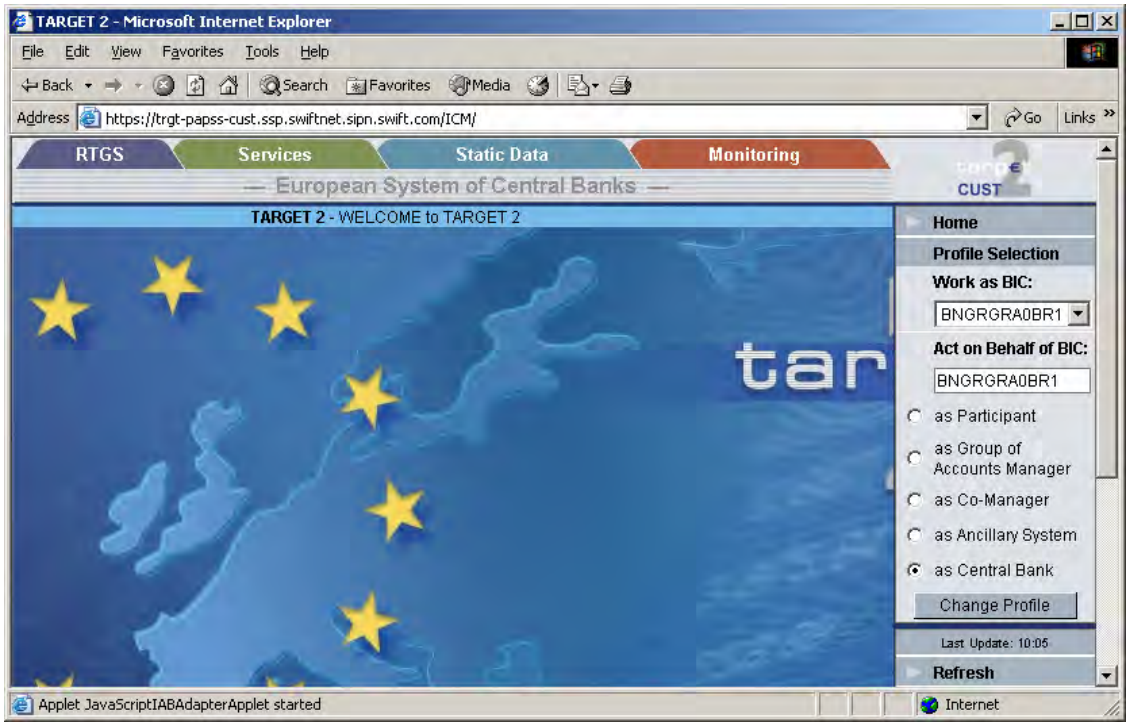
5. Στο δεύτερο αυτό παράθυρο (IAB Started) και στο πεδίο “Address” πληκτρολογούμε τη διεύθυνση για το Test περιβάλλον του Target2 / ICM:

   https://trgt-papss-cust.ssp.swiftnet.sipn.swift.com και <Enter> ή: “Go”

6. Στο αναδυόμενο (pop-up) παράθυρο επιλέγουμε το επιθυμητό πιστοποιητικό – Browser Certificate (πιθανότατα θα είναι μόνο ένα, με όνομα της μορφής: %N, όπου N ακέραιος) και πατάμε “OK”. Μας ζητείται η εισαγωγή του password για το Certificate (passwd-2), το οποίο και πληκτρολογούμε.

7. Κατόπιν εμφανίζεται η αρχική οθόνη του TARGET2 και ζητείται αμέσως η εισαγωγή του “SWIFTAlliance WebStation password”. **ΠΡΟΣΟΧΗ:** εδώ πληκτρολογούμε το password του SN-user που έχει εκκινήσει το WebStation (δηλ. το passwd-1). Εάν είναι ενεργοποιημένη η λειτουργία της επιβεβαίωσης (confirmation), απαιτείται “OK” και στο σχετικό αναδυόμενο (pop-up) παράθυρο.

8. Τέλος εμφανίζεται η λεγόμενη “οθόνη υποδοχής (Welcome Screen)” του Target2, η οποία έχει την παρακάτω μορφή:



Ο χρήστης είναι πλέον σε θέση να εκτελέσει όλες τις εργασίες, για τις οποίες είναι εξουσιοδοτημένος. Οι σχετικές εξουσιοδοτήσεις του κάθε χρήστη καθορίζονται στα πλαίσια του οργανισμού-εταιρείας, περιγράφονται δε αναλυτικά στα αντίστοιχα εγχειρίδια του Target2. Η υλοποίηση των ως άνω εξουσιοδοτήσεων γίνεται μέσω του μηχανισμού RBAC (Role-Based Access Control) του SWIFTNet, η δε εκχώρησή τους στους αντίστοιχους χρήστες είναι αρμοδιότητα του SWIFTNet Security Officer (SO) του οργανισμού-εταιρείας.

Εναλλακτική μορφή λειτουργίας του WebStation

Μια απλούστερη μέθοδος χρήσης του WebStation, εφ’όσον η μόνη λειτουργία που απαιτείται είναι το Browsing (και μόνον αυτό), είναι η εξής:

Δημιουργούμε στην επιφάνεια εργασίας ένα εικονίδιο-συντόμευση (shortcut), που να δείχνει στην εξής διαδρομή:

C:\SWIFTAlliance\WebStation\iab\HTTPAdJClient.exe

Στη συνέχεια, ο χρήστης μπορεί να εκκινήσει τη σύνδεση με το ICM κάνοντας διπλό click στο ως άνω εικονίδιο-συντόμευση, παρακάμπτοντας κάποια από τα βήματα που απαιτούνται στην πλήρη διαδικασία εκκίνησης, όπως αυτή έχει περιγραφεί σε προηγούμενη παράγραφο. Εννοείται ότι όλοι οι έλεγχοι ασφαλείας (User-names, Passwords κλπ) εξακολουθούν να είναι απαραίτητοι.

Προδιαγραφές για SWIFTNet passwords

Ελάχιστο μήκος: 8 χαρακτήρες

Επιτρεπόμενοι χαρακτήρες: Κεφαλαία λατινικά, μικρά λατινικά, αριθμ.ψηφία

Υποχρεωτική παρουσία: Ενα κεφαλαίο, ένα μικρό, ένα ψηφίο.

ΠΡΟΕΤΟΙΜΑΣΙΑ ΓΙΑ ΤΗΝ ΛΕΙΤΟΥΡΓΙΑ ΣΕ "FIN-Copy Mode" / Y-Copy

Η διακίνηση FIN μηνυμάτων στο περιβάλλον του Target2 στηρίζεται στην ύπαρξη, στα πλαίσια του SWIFT, μιας κλειστής ομάδας – CUG (Closed User Group), με κωδικό TGT, μέλη της οποίας είναι οι συμμετέχουσες Τράπεζες, ενώ ως κεντρικός φορέας-οργανισμός (Central Institution) λειτουργεί η ίδια η SSP. Η λειτουργία του FIN-Copy/Y-Copy, όπως είναι γνωστό, ορίζει εν περιλήψει ότι κατά την αποστολή ενός FIN μηνύματος από τον αποστολέα (A) στον παραλήπτη (B) παρεμβάλλεται ένας κεντρικός φορέας (K), ο οποίος λαμβάνει πρώτος το μήνυμα και, εφόσον το "εγκρίνει", το προωθεί προς τον παραλήπτη.

Προς το παρόν, επειδή δεν έχει ακόμη ολοκληρωθεί πλήρως η μετάβαση του SWIFTNet σε "καθαρό" PKI περιβάλλον, υπάρχει η απαίτηση για διμερή ανταλλαγή κλειδών (Bilateral Key Exchange – BKE), στα πλαίσια του Target2. Συγκεκριμένα, κάθε συμμετέχουσα Τράπεζα πρέπει να ανταλλάξει κλείδες με την κοινή πλατφόρμα (SSP), η οποία έχει κωδικό (BIC8): **TRGTXEP0** (Test περιβάλλον). Η ανταλλαγή αυτή εκτελείται με πρωτοβουλία (Initiation) της SSP. Δεν απαιτείται ανταλλαγή κλειδών μεταξύ των συμμετεχουσών Τραπεζών.

Επιπλέον, απαιτείται η εγκατάσταση, ρύθμιση και ενεργοποίηση της λειτουργίας FIN-Copy στο περιβάλλον του αντίστοιχου CBT (Computer-Based Terminal), από το οποίο αποστέλλονται τα FIN μηνύματα. Στην περίπτωση που υπάρχει λογισμικό SAA (SWIFT Alliance Access), το οποίο λειτουργεί ως CBT, τα απαιτούμενα βήματα είναι συνοπτικά τα εξής (βλ. και: FIN-Copy Release Letter και SWIFTNet-document: SAA 6.0 System Management Guide – Chapter 7):

1. Διασφάλιση ότι το σχετικό λογισμικό περιλαμβάνει υποστήριξη για το λεγόμενο "Pre-agreed MAC". Το SAA version 6.0 ενσωματώνει την αντίστοιχη δυνατότητα, ενώ οι αποδεκτές προηγούμενες εκδόσεις ήταν η SAA 5.5.60 ή SAA 5.9

2. Μεταφορά (Download) από το Site του SWIFT του σχετικού FIN-Copy "patch": https://www2.swift.com/pdc (login required) – επιλογή του πρόσφατου FIN-Copy patch για το συγκεκριμένο λειτουργικό σύστημα (AIX, Solaris, Windows) στο οποίο λειτουργεί το SAA.

3. Εξαγωγή (extract) του service configuration file: **TTTGT.fcp** (for Test & Training Target2)

4. (Επαν-) Εκκίνηση του SAA σε "**House Keeping**" mode

5. Εκκίνηση του “**SWIFT Support**” Application

6. Επιλέγουμε “Value-added Services” από το “View Menu”

7. Επιλέγουμε “Install”

8. Στο σχετικό path συμπληρώνουμε τη διαδρομή που οδηγεί στο σημείο όπου έχουμε αποθηκεύσει το file: **TTTGT.fcp** και πατάμε “Install”.

9. Στη συνέχεια, από το “Value-added Services” (στο View Menu), επιλέγουμε **TGT (T&T)** Service και κατόπιν επιλέγουμε “Activate”. Το σχετικό πεδίο “State” λαμβάνει την τιμή: active.

Σημ. Η εκτέλεση των βημάτων έως εδώ, εξασφαλίζει ότι η εγκατάσταση του FIN-Copy είναι επιτυχής.

10. Με το SAA σε “House Keeping” mode και από το SWIFT Support Application, επιλέγουμε “Value-added Services” (στο View Menu), επιλέγουμε **TGT (T&T)** Service και, εν συνεχεία, “De-activate”. Το σχετικό πεδίο “State” λαμβάνει την τιμή: inactive.

11. Συσχέτιση – Assign του FIN-Copy σε destination(s) / BIC8(s): Με το SAA σε “House Keeping” mode, από το SWIFT Support Application: “Value-added Services” (από View Menu), επιλέγουμε το **TGT (T&T)** Service και, εν συνεχεία: Destinations. Κατόπιν μεταφέρουμε, ένα προς ένα, τα BIC8 που θέλουμε να συμμετέχουν σε FIN-Copy, από την κατηγορία “Available” στην κατηγορία “Selected” και αποθηκεύουμε τις αλλαγές. (Προς το παρόν δεν απαιτείται RMA Authorisation, οπότε το σχετικό πεδίο παραμένει με την ένδειξη “Not Required”).

12. Ενεργοποιούμε εκ νέου το FIN-Copy, όπως στο βήμα 9. πιο πάνω

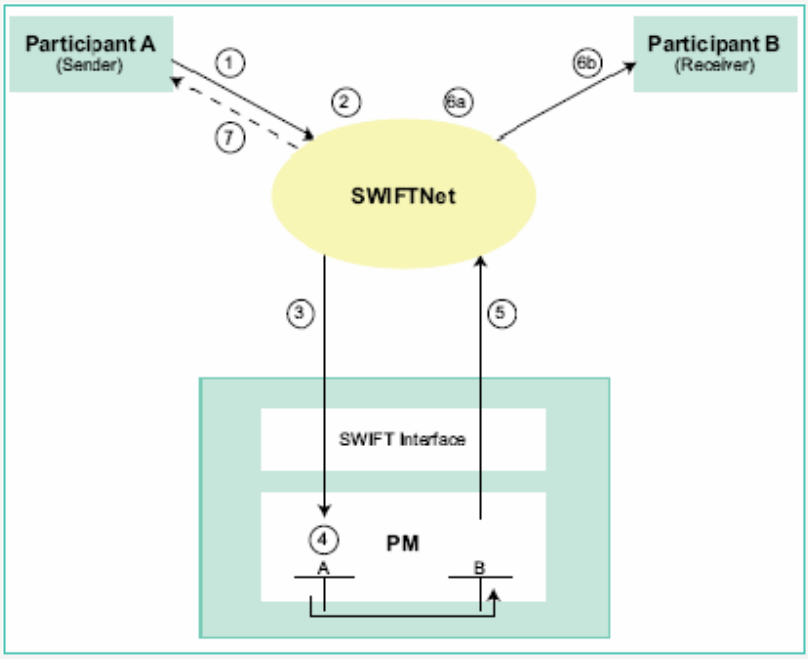
13. Επαναφέρουμε το SAA σε κανονική λειτουργία (Operational mode)

Ανακεφαλαιωτικά, τα κύρια βήματα για το FIN-Copy είναι:

- Download FIN-Copy
- Install FIN-Copy
- Activate FIN-Copy
- De-activate FIN-Copy
- Assign FIN-Copy to destination(s) – BIC8(s)
- Activate FIN-Copy

ΠΑΡΑΔΕΙΓΜΑ ΛΕΙΤΟΥΡΓΙΑΣ FIN-Copy / Y-Copy

The following slide depicts the processing of a payment from a direct PM participant in favour of another direct PM participant:



The following table describes the processing of a direct debit generated by a direct PM participant (A) debiting another direct PM participant (B):

Step	Description
1	The direct PM participant A (Sender) generates a direct debit debiting the RTGS account of the direct PM participant B (Receiver) and addresses B in the application header of the direct debit.
2	The payment is temporarily stored by SWIFT.
3	A settlement request (MT 096) with a full copy is generated by SWIFT and forwarded to the PM.
4	The direct debit has to pass several validations (SWIFT syntax, application oriented entry checks, availability of sufficient cover and sufficient direct debit maximum amounts etc.) before the direct debit is debited on the RTGS account of B and simultaneously credited on the RTGS account of A.
5	A settlement confirmation (MT 097) is generated in the PM and forwarded to SWIFT.
6a	The settlement confirmation and the original direct debit are matched and the booking time is added to the original direct debit in the SWIFT network.
6b	The direct debit message is forwarded to B.
7	Optional: A can receive a sender notification (MT 012) which also contains the booking time.

ΠΙΝΑΚΑΣ ΕΡΜΗΝΕΙΑΣ ΣΥΝΤΟΜΟΓΡΑΦΙΩΝ

BIC	Bank Identifier Code
BKE	Bilateral Key Exchange
CUG	Closed User Group
DN	Distinguished Name
ECB	European Central Bank
HAM	Home Accounting Module
ICM	Information and Control Module
MAC	Message Authentication Code
MT	Message Type
NCB	National Central Bank
PAPPS	Payment and Accounting Processing Services
PKI	Public Key Infrastructure
PM	Payment Module
RBAC	Role-Based Access Control
RTGS	Real-Time Gross Settlement
SAB	SWIFTAlliance WebStation
SAG	SWIFTAlliance Gateway
SAS	SWIFTAlliance Starter Set
SIPN	Secure IP Network
SNL	SWIFTNetLink
SSP	Single Shared Platform
TARGET	Trans-European Automated Real-Time Gross Settlement Express Transfer
XML	eXtensible Markup Language