AnaSys
finest financial messaging

SWIFT Customer Security Programme

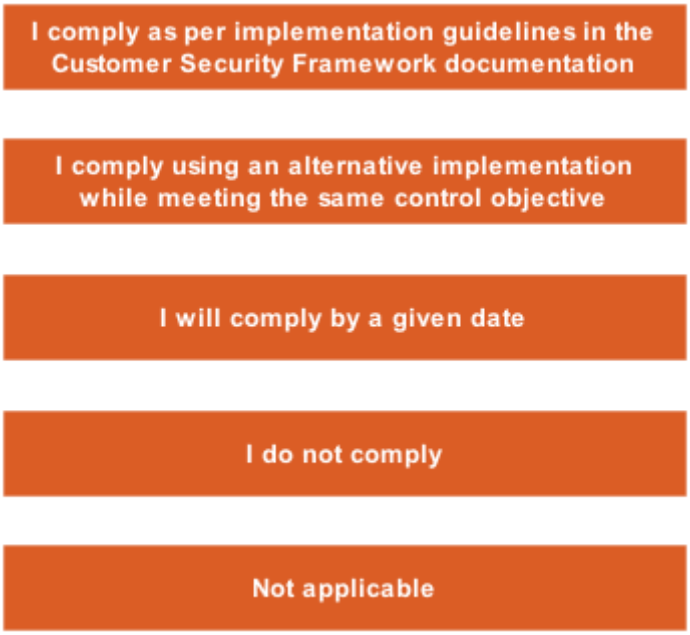
Das SWIFT Customer Security Programme (kurz: CSP) wurde ins Leben gerufen um die lokale SWIFT-Infrastruktur gegen Cyberattacken zu sichern. SWIFT hat die lokale Umgebung beim Kunden als wichtigsten Angriffspunkt für Cyber-Attacken ausgemacht. Das CSP soll eine einheitliche, hohe Sicherheit bei allen SWIFT-Nutzern gewährleisten.

Das SWIFT Customer Security Programme besteht aus 16 verpflichtenden Kontrollen und 11 vorgeschlagenen, nicht zwingenden Kontrollen. SWIFT rät dazu diese vorgeschlagenen Kontrollen ebenfalls zu erfüllen, um einen umfassenden Schutz vor Cyberattacken zu erhalten. Zusätzlich soll das CSP in den nächsten Jahren ausgebaut werden und es mehr verpflichtende Kontrollen gibt.

Es gibt verschiedene Architekturmodelle, in die die Kunden ihre Infrastruktur einordnen müssen. Für alle Kunden im Service Bureau ist das A3, wenn Sie die automatische Schnittstelle (Hostlink) einsetzen.

Jeder SWIFT-Kunde muss für jeden Live-BIC eine gesonderte Self-Attestation (Selbstbescheinigung) erbringen. Diese Selbstbescheinigung wird über das KYC-Portal (Know your Customer) unter dem Punkt KYC-SA erfolgen und ist bereits verfügbar.

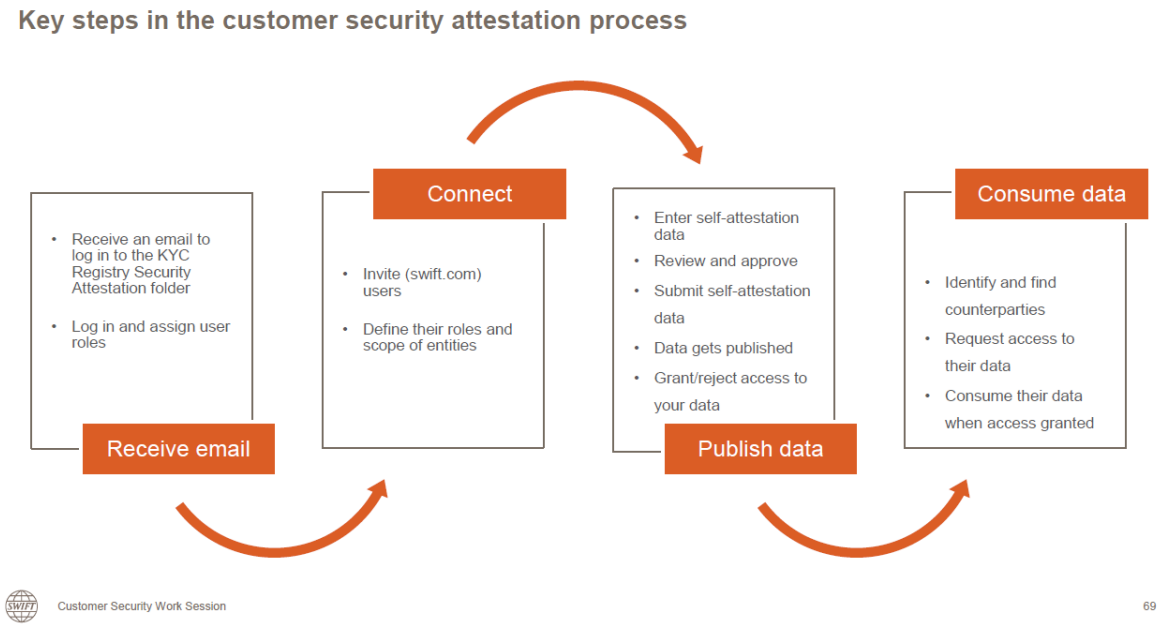
Die Antwortmöglichkeiten sind dabei folgende:



SWIFT wird nach der Abgabe der Selbstbescheinigung eine Prüfung der Antworten durchführen. Diese ist aber rein formal (sind alle Antworten enthalten, Stimmen die Adressangaben, etc.) Eine Überprüfung oder Validierung der Antworten wird es vorerst nicht geben. SWIFT schreibt vor, dass die Self-Attestation bis Ende 2017 erfolgen muss, ansonsten wird SWIFT diese Tatsache an die zuständige Aufsichtsbehörde melden. In dieser ersten Selbstbescheinigung bis Ende 2017 ist es nicht

notwendig allen Kontrollvorgaben zu entsprechen, es wird nur überprüft, ob überhaupt eine Self-Attestation durchgeführt wurde. Im zweiten Schritt bis Ende 2018 verlangt SWIFT dann den Kontrollen zu entsprechen, das heißt bei allen zwingend zu erfüllenden Richtlinien, muss „I comply“ angekreuzt werden.

Die somit gewonnen Antworten und Daten werden zentral bei SWIFT gespeichert, aber die Kunden behalten die Hoheit über diese Daten. Jeder andere SWIFT Kunde, der Einsicht nehmen möchte, muss den Dateneinreicher fragen, ob er Zugriff auf die Daten erhält. Dieser kann dann den Zugang gewähren oder ablehnen.



Weitere wichtige Informationen gibt es durch verschieden Kanäle:

- Die Dokumente “SWIFT Customer Security Controls Framework” und “SWIFT Customer Security Controls Policy” aufmerksam studieren
- Die Trainingsplattform „SWIFTSmart“ hält viele Module bereit, insbesondere detaillierte Informationen zu jedem zwingenden Kontrollpunkt
- Auf MySWIFT gibt es ein Portal mit “how-to“-videos, FAQs und einer Knowledge Base
- Auf den CSP Seiten auf swift.com werden News und Programm-Updates bekannt gegeben
- Das SWIFT ISAC Portal gibt Auskunft über aktuelle Sicherheitsbedrohungen