RANDORISEC

乱取り

SWIFT

Customer Security Programme

L'origine et le périmètre

1 La genèse

SWIFT en quelques dates

1973 : création d'un coopérative bancaire en Belgique

1977 : ouverture du réseau – envoi du premier message

1993 : 100e pays connecté

2016 : Cyber-attaque de la Banque Centrale du Bangladesh

Gottfried Leibbrandt
SWIFT CEO (de 2012 à 2019)

?

Les clients de SWIFT

Le Customer Security Programme

ISO International Organization for Standardization

ISO 27002
Information Technology
Security Techniques
Code of Practice for
Information Security Controls

NIST

PCI DSS COMPLIANT


SWIFT Customer Security Controls Framework 1.0

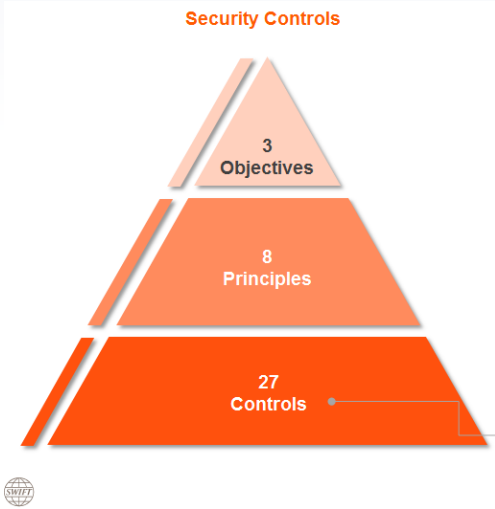
Customer Security Programme

Detailed Description

This document establishes a set of mandatory and advisory security controls for SWIFT users. Mandatory security controls build on existing guidance and establish a security baseline for the entire user community. Advisory controls are optional good practices that SWIFT recommends each user implement in their environment.

31 March 2017

Le Customer Security Programme



CSP Security Controls Framework

Secure Your Environment	1.	Restrict Internet access
	2.	Segregate critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

- *Applicable to all customers and their SWIFT infrastructure*
- *Mapped against recognised international standards – NIST, PCI-DSS and ISO 27002*
- *16 controls are mandatory, 11 are advisory*

Que faire ?


BANK


SWIFT


BANK


SWIFT


BANK

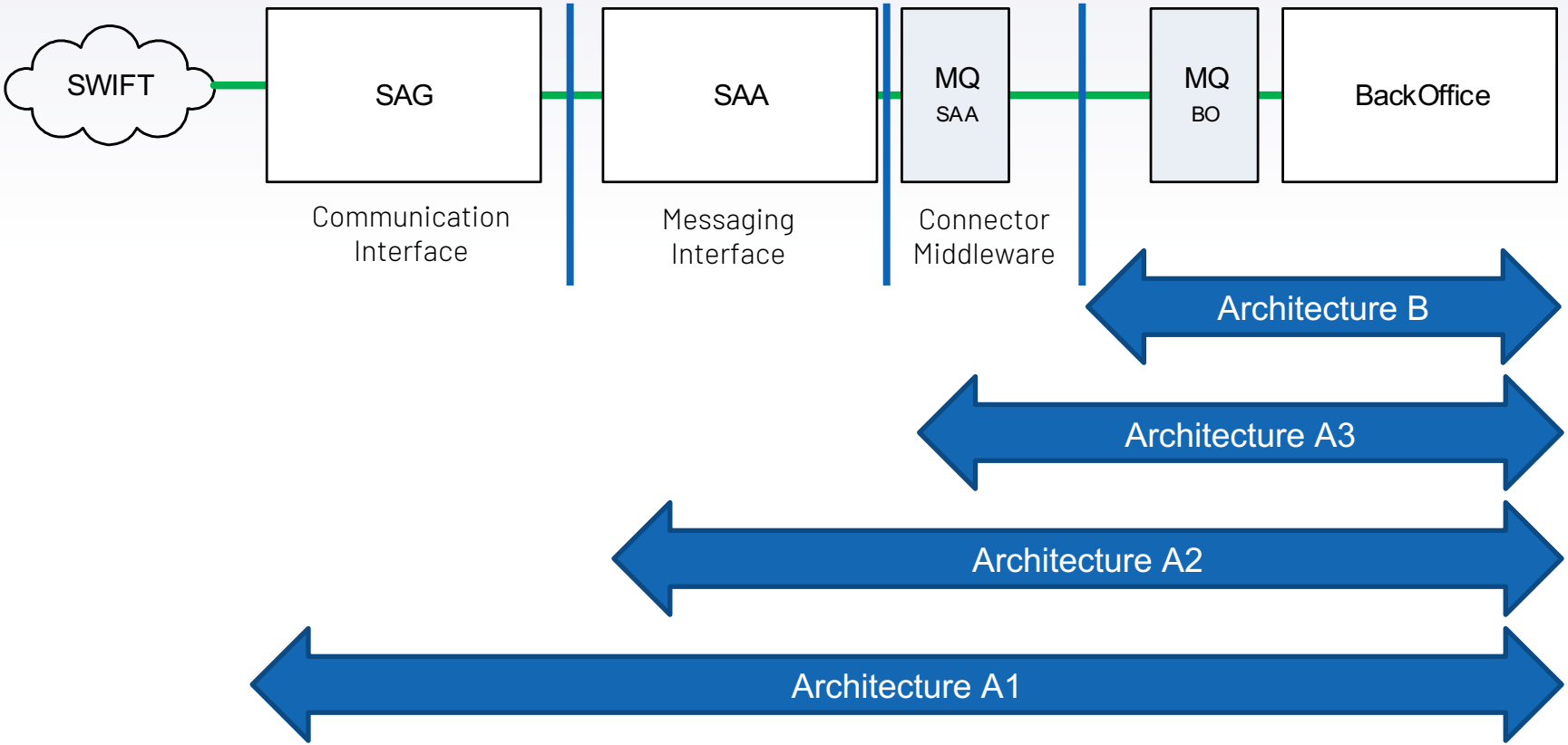

WORLD NEWS
NEWSPAPER TEMPLATE VECTOR EPS
«Lorem ipsum dolor sit amet, movet doming ne ius. Ne tale»


KYC

2

En détail

Quelle architecture ?



Le Customer Security Programme

1 Restrict Internet Access & Protect Critical Systems from General IT Environment
- 1.1 SWIFT Environment Protection
- 1.2 Operating System Privileged Account Control
- 1.3 Virtualisation Platform Protection
- 1.4A Restriction of Internet Access

2 Reduce Attack Surface and Vulnerabilities
- 2.1 Internal Data Flow Security
- 2.2 Security Updates
- 2.3 System Hardening
- 2.4A Back Office Data Flow Security
- 2.5A External Transmission Data Protection
- 2.6 Operator Session Confidentiality and Integrity
- 2.7 Vulnerability Scanning
- 2.8A Critical Activity Outsourcing
- 2.9A Transaction Business Controls
- 2.10 Application Hardening
- 2.11A RMA Business Controls

3 Physically Secure the Environment
- 3.1 Physical Security

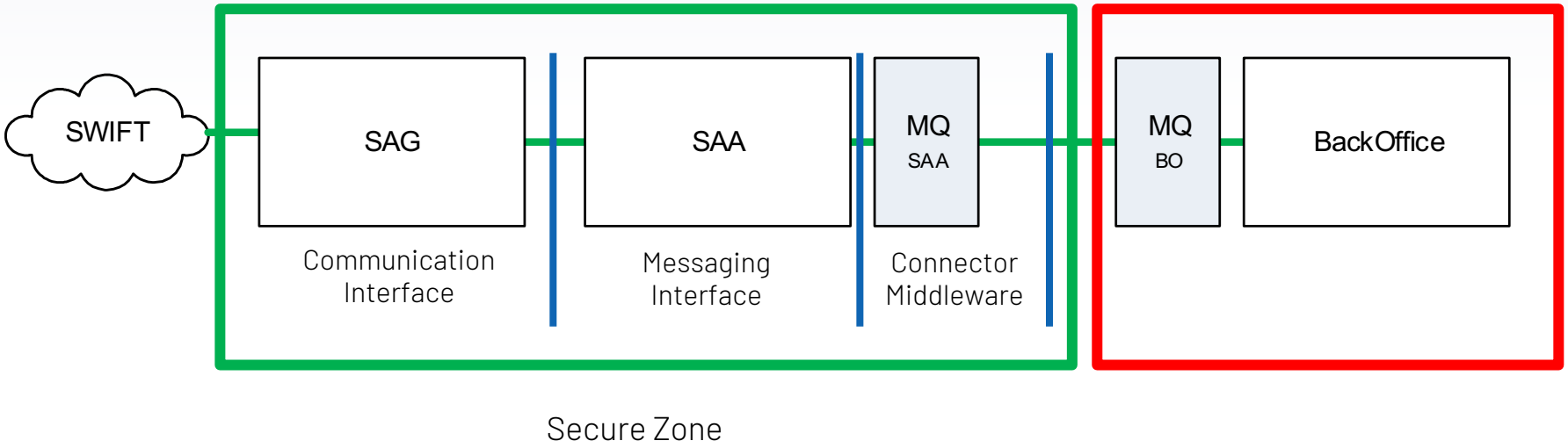
4 Prevent Compromise of Credentials
- 4.1 Password Policy
- 4.2 Multi-factor Authentication

5 Manage Identities and Segregate Privileges
- 5.1 Logical Access Control
- 5.2 Token Management
- 5.3A Personnel Vetting Process
- 5.4 Physical and Logical Password Storage

6 Detect Anomalous Activity to Systems or Transaction Records
- 6.1 Malware Protection
- 6.2 Software Integrity
- 6.3 Database Integrity
- 6.4 Logging and Monitoring
- 6.5A Intrusion Detection

7 Plan for Incident Response and Information Sharing
- 7.1 Cyber Incident Response Planning
- 7.2 Security Training and Awareness
- 7.3A Penetration Testing
- 7.4A Scenario Risk Assessment

Le grand principe : une zone sûre



Isolation technique

- Serveurs dédiés
- Ségrégation du reste du SI
- LDAP dédiés

Physiquement sûr

- Datacenters protégés
- Serveur sans nom

Frontières protégées

- Revue des règles FW
- Revue des logs FW

Accès Sécurisés

- Rupture de protocole (serveurs de rebond)
- Pas de lien Internet
- Flux chiffrés
- Protocoles à jour

Accès Contrôlés

- Vérification des utilisateurs
- Compte à privilèges désactivés
- Politique de mot de passe robustes
- Double Authentification

Durcissement

- Niveau OS
- Niveau applicatif

Supervision active

- Suivi des actions personnelles
- Logs collectées
- Usecases SIEM

Environnement sûr

- Logiciels à jour (OS & applications)
- Protection antimalware à jour (serveurs et postes)
- Validation de l'intégrité (fichiers et BDD)

Vérifications poussées

- Scans de vulnérabilité
- Test de pénétration
- Détections d'intrusion

Validation fonctionnelle

- Validation des flux échangés
- Validation des contreparties

Suivi du personnel

- Criblage personnel
- Formation régulière

Crise anticipée

- Procédure de Continuité d'Activité
- Procédure en cas de cybermenace
- Exercice de mise en situation

3

Et après ?

Le CSP au jour le jour

Validation par audit

- Interne
- Externe

Travail au quotidien

- Collecte de preuve
- Prise en compte dans les projets

Une mise à jour annuelle

- Nouveaux chapitres
- Passage en obligatoire
- Discussion dans les groupes de Place

Gestion des attestations

- Demande aux contreparties
- Politique de réponse
- Conformité aux régulateurs, aux systèmes de place (TARGET 2, CHAPS, etc.)

MERCI!

Des questions?

randorisec.fr

blog.randorisec.fr

@RandoriSec

Crédits

Merci aux personnes qui ont mis à disposition ces ressources gratuitement :

- Modèle de présentation PowerPoint par SlidesCarnival
- Photographie par Pixabay
- Source documentaire : SWIFT.com