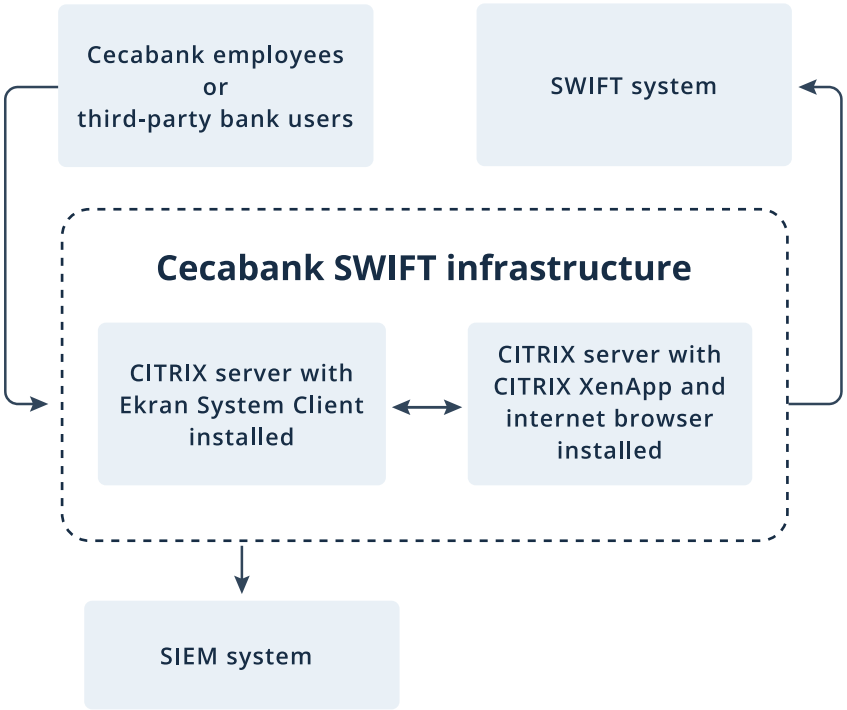
CASE STUDY

Cecabank Ensures SWIFT CSP Compliance with Help of Ekran System

THE CHALLENGE

Any organization that uses SWIFT services has to comply with security controls described in the SWIFT Customer Security Programme (CSP). To maintain SWIFT CSP compliance and improve their security, our customer needed to reduce the risk of SWIFT account compromise and detect the potential use of compromised SWIFT credentials.

Bank users access the SWIFT environment via two Citrix servers and Citrix XenApp. Therefore, Cecabank decided to record all successful logins to Citrix instances. They also wanted to be able to upload SWIFT access logs to their security information and event management (SIEM) system.



Cecabank was searching for a reliable partner to help them comply with updated SWIFT CSP requirements. After studying the market, they decided to go with Ekran System.

THE CUSTOMER

cecabank

Cecabank, S.A. is a Spanish wholesale bank with representative offices in the UK, Hong Kong, France, and Germany. Cecabank offers various services, from securities to cash management to banking.

To support international infrastructure, ensure the quality of their services, and interact with third-party banks, Cecabank works with the SWIFT network and services.

CECABANK's OBJECTIVES

- Establish visibility in the SWIFT environment
- Detect the use of compromised SWIFT credentials
- Upload SWIFT access logs to their SIEM

Customer's need	The result	Our offer
Establish visibility in the SWIFT environment	Clear understanding of who does what in the SWIFT environment	SWIFT user activity monitoring and recording
		Recording of logging attempts with optical character recognition algorithm
Detect the use of compromised SWIFT credentials	Ability to prevent or stop attacks in the SWIFT environment at early stages	Real-time alerts on suspicious actions and security violations
Upload SWIFT access logs to the SIEM	Enable easy and efficient data analysis	Forwarding of SWIFT access logs to the customer's SIEM system

THE RESULT

Deploying Ekran System helped our customer to:

- **Gain a clear understanding of who does what in their SWIFT environment**
- **Prevent or stop attacks in the SWIFT environment at early stages**
- **Analyze SWIFT access logs easily via their SIEM**

> *Ekran customized some of their functionality to help us solve our security task. Now, monitoring and auditing users accessing the SWIFT network through our environment is much easier.*

Security Architect,
Cecabank

HOW WE DID IT

Financial and banking organizations often choose Ekran System for our robust selection of privileged access management features, multi-factor authentication, password management, rich user activity monitoring, and many other capabilities.

Cecabank fulfilled their needs and confirmed compliance with SWIFT CSP requirements by leveraging the following Ekran System features:

- **Real-time session views** in a YouTube-like player give a comfortable way to see how employees work with sensitive data and critical systems. In case an alert is triggered, security officers can investigate in real time whether a user is performing malicious actions.
- **Recording of logging attempts with an optical character recognition (OCR) algorithm.** Keeping a log of all attempts to connect to the SWIFT environment is one of the key SWIFT CSP requirements. To ensure Cecabank's compliance, the Ekran System team implemented an OCR algorithm that recognizes and logs usernames submitted for SWIFT login. This way, users logged in to the SWIFT network can easily be associated with users logged in to the bank's system.
- **SWIFT user activity monitoring and recording.** With 24/7 monitoring and recording of user activity, Cecabank's security officers know who does what inside the SWIFT environment. They can conveniently search for any type of activity on their Citrix servers and review suspicious user sessions via a built-in YouTube-like player.
- **Real-time alerts on suspicious actions and security violations.** Security incidents in the SWIFT environment require a fast response. Cecabank's security officers can ensure this with real-time alerts on suspicious user activity or events. Using these alerts, they can analyze an incident and block the flagged user or application if needed.
- **Forwarding of SWIFT access logs to Cecabank's SIEM system.** Gathering all the security logs within one system allows Cecabank's IT administrators to streamline their work and centralize data management. That's why the ease of integrating Ekran System with the deployed SIEM is one of the most important benefits for our customer.

During our partnership, Cecabank also noted enterprise-friendly features of Ekran System like high availability mode, remote client deployment and updates, and 24/7 support. That's why our pilot deployment project turned into a long-term partnership that we hope will continue for years.