SWIFT CUSTOMER SECURITY PROGRAMME (CSP) COMPLIANCE WITH EKRAN SYSTEM® SOFTWARE

A detailed technical brief showing how Ekran System features map to SWIFT Customer Security Controls and presenting possible deployment schemes

Customers Who Trust Us
SWIFT CUSTOMER SECURITY PROGRAMME (CSP)

To answer the growing threat landscape, the SWIFT organization has developed and introduced a formalized security program for its customers. Starting December 2017, any financial organization that uses SWIFT must comply with a set of 16 mandatory security controls and take all reasonable efforts to meet 11 advisory security controls that together comprise the **SWIFT Customer Security Controls Framework**. Compliance is to be confirmed every 12 months.

Aiming at reinforcing SWIFT customers’ cyber security and preventing fraud, the Framework translates the industry best security practices and guidelines into three key objectives (Secure Your Environment, Know and Limit Access, Detect and Respond). These main objectives are further detailed in groups of technical, organizational, and educational security controls.

<table>
<thead>
<tr>
<th>Objective</th>
<th>Secure Your Environment</th>
<th>Know and Limit Access</th>
<th>Detect and Respond</th>
</tr>
</thead>
<tbody>
<tr>
<td>Principles (and corresponding security control groups)</td>
<td>1. Restrict internet access and protect critical systems from the general IT environment</td>
<td>4. Prevent compromise of credentials</td>
<td>6. Detect anomalous activity to systems or transaction records</td>
</tr>
<tr>
<td></td>
<td>2. Reduce the attack surface and vulnerabilities</td>
<td>5. Manage identities and segregate privileges</td>
<td>7. Plan for incident response and information sharing</td>
</tr>
<tr>
<td></td>
<td>3. Physically secure the environment</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
BUILD YOUR SWIFT CSP COMPLIANCE WITH EKRAN SYSTEM®

The Ekran System® insider threat protection platform is your powerful ally in adopting SWIFT Customer Security Controls.

This robust and flexible agent-based software supports a wide range of operating systems, configurations, and network architectures, including desktops, servers, and jump servers. It supports both physical and virtual infrastructures. With Ekran System, you can control access to your secure zone and identities of your users, monitor and record any activity within it, get alerted to suspicious actions, and enable incident response.

See deployment schemes

KEY FEATURE GROUPS

Access Control
- Privileged account and session management (PASM)
- Temporary and one-time credentials
- Manual login approval
- Ticketing system integration with purpose validation
- Password vault

Identity Control
- Multi-factor authentication
- Secondary authentication to identify users of shared and built-in accounts

Session Monitoring and Recording
- Terminal, remote, and local session recording in indexed video format
- Searchable multi-layer text index (URLs, commands, keystrokes, applications, connected devices, etc.)
- Continuous monitoring with optional record filtering (by user, application, or URL)
- Forensic export of records

Real-time Alerting and Incident Response
- Template-based and fully customizable alerts on anomalous, suspicious, and high-risk events
- Alerts delivered in real time accompanied with relevant event context
- Manual and automated incident response actions including user warning and blocking, device blocking, and process termination

See detailed security control – feature mapping
EKRAN SYSTEM® - A FLEXIBLE AND SECURE SOLUTION

Supported Platforms

- Windows
- MacOS
- Linux
- UNIX®
- VMware
- Citrix
- X

Secure Solution

- Application hardening
- Detailed internal action logging
- Highly-protected data storage
- Encrypted communication channels

Flexible Deployment

- High-availability mode
- Multi-tenant and single-tenant modes
- Integration with SIEM and ticketing systems
- Online and offline updates, automated client updates
- Self-monitoring system dashboard
- Easily scalable deployments
## DETAILED SECURITY CONTROLS AND EKRAN SYSTEM® FEATURES MAPPING

<table>
<thead>
<tr>
<th>Security Control</th>
<th>Objective</th>
<th>Ekran System Role</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Restrict Internet Access and Protect Critical Systems from General IT Environment</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 1.1 SWIFT Environment Protection | Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment. | Ekran System allows security teams to protect the SWIFT secure zone by setting up a jump server inside the secure zone and restricting access to the server only to trusted administrators. All corresponding Ekran System management components including the password vault can be deployed inside the secure zone, and authentication service segregation can be implemented.

Access to resources located inside the secure zone can further be protected by installing Ekran System Clients on them, allowing security officers to control user activity more granularly, for instance by blocking certain actions or applications. Installed clients provide verbose logging and detection capabilities. |
| 1.2 Operating System Privileged Account Control | Restrict and control the allocation and usage of administrator-level operating system accounts. | Ekran System provides a secondary authentication feature to identify users of shared accounts, such as built-in administrator-level operating system accounts, based on individual credentials. This allows not only detailed logging but also restricting and permitting access to shared accounts for specific users.

Ekran System provides two options for emergency access, avoiding use of built-in accounts: one-time passwords and login with mandatory manual approval from a security officer. An additional level of control by purpose can be arranged using ticketing system integration, which adds validation against open tickets.

Verbose in-depth activity monitoring delivered by Ekran System for each session started within the secure zone allows a security team to monitor all administrator-level activity, including sudo commands and the content of executed scripts. |
| 1.3A Virtualisation Platform Protection | Secure virtualisation platform and virtual machines (VMs) hosting SWIFT-related components to the same level as physical systems. | Ekran System provides out-of-the-box support for virtual environments, delivering its full functionality for virtual machines and virtualization platforms. Additional features such as integration into golden images and dynamic license pools simplify maintenance. |
| **2. Reduce Attack Surface and Vulnerabilities** |                                                                           |                                                                                  |
| 2.1 Internal Data Flow Security | Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC. | n/a |
| 2.2 Security Updates | Minimise the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk. | n/a |
## Security Control Objectives

<table>
<thead>
<tr>
<th>Security Control</th>
<th>Objective</th>
<th>Ekran System Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.3 System Hardening</td>
<td>Reduce the cyber attack surface of SWIFT-related components by performing system hardening.</td>
<td>n/a</td>
</tr>
<tr>
<td>2.4A Back-office Data Flow Security</td>
<td>Ensure the confidentiality, integrity, and mutual authenticity of data flows between back office (or middleware) applications and connecting SWIFT infrastructure components.</td>
<td>n/a</td>
</tr>
<tr>
<td>2.5A External Transmission Data Protection</td>
<td>Protect the confidentiality of SWIFT-related data transmitted and residing outside of the secure zone.</td>
<td>n/a</td>
</tr>
<tr>
<td>2.6 Operator Session Confidentiality and Integrity</td>
<td>Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure.</td>
<td>n/a</td>
</tr>
<tr>
<td>2.7 Vulnerability Scanning</td>
<td>Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process and act upon results.</td>
<td>n/a</td>
</tr>
<tr>
<td>2.8A Critical Activity Outsourcing</td>
<td>Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.</td>
<td>Ekran System allows security teams to grant secure third-party access to the secure zone without revealing actual access credentials via its PASM functionality. All corresponding access permissions are temporary and can be reviewed, continued, or revoked. A one-time password mechanism can be used to provide one-time access. Ticketing system integration enables additional validation of the purpose of access. For close contractor monitoring, access can be set up with mandatory manual login approval from a security officer with subsequent real-time video supervision.</td>
</tr>
<tr>
<td>2.9A Transaction Business Controls</td>
<td>Restrict transaction activity to validated and approved counterparties and within the expected bounds of normal business.</td>
<td>n/a</td>
</tr>
<tr>
<td>2.10A Application Hardening</td>
<td>Reduce the attack surface of SWIFT-related components by performing application hardening on the SWIFT-certified messaging and communication interfaces and related applications.</td>
<td>n/a</td>
</tr>
</tbody>
</table>

### 3. Physically Secure the Environment

<table>
<thead>
<tr>
<th>Security Control</th>
<th>Objective</th>
<th>Ekran System Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1 Physical Security</td>
<td>Prevent unauthorised physical access to sensitive equipment, workplace environments, hosting sites, and storage.</td>
<td>Ekran System protects servers from unauthorized physical access by blocking access to or restricting the use of USB ports. With a whitelisting option, specific USB devices, such as hardware tokens, can be allowed. Ekran System reliably monitors, alerts about, and blocks both USB storage devices and other USB devices of any nature.</td>
</tr>
</tbody>
</table>
### DETAILED SECURITY CONTROLS AND EKRAN SYSTEM® FEATURES MAPPING

<table>
<thead>
<tr>
<th>Security Control</th>
<th>Objective</th>
<th>Ekran System Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>4. Prevent Compromise of Credentials</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.1 Password Policy</td>
<td>Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.</td>
<td>n/a</td>
</tr>
<tr>
<td>4.2 Multi-factor Authentication</td>
<td>Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication.</td>
<td>To enhance authorization credibility, Ekran System supports time-based one-time passwords delivered via a mobile app when logging in to the operator PC. This gives an additional layer of protection against credential theft.</td>
</tr>
<tr>
<td>5. Manage Identities and Segregate Privileges</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1 Logical Access Control</td>
<td>Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts.</td>
<td>To enhance authorization credibility, Ekran System provides a broad set of access control tools for both privileged and ordinary users. It includes temporary credential management on a jump server via PASM functionality coupled with a secure password vault and automated credential provisioning. One-time passwords are generated by security administrators for one-time access scenarios. Access to a secure endpoint is given only after manual approval of this login from a security administrator who can monitor the initiated session in real time. The purpose of access is validated via integration with a ticketing system. These tools allow a security team to implement best practices such as segregation of duties, four-eye control, the least privilege principle, and purpose-based access.</td>
</tr>
<tr>
<td>5.2 Token Management</td>
<td>Ensure the proper management, tracking, and use of connected hardware authentication tokens (if tokens are used).</td>
<td>n/a</td>
</tr>
<tr>
<td>5.3A Personnel Vetting Process</td>
<td>Ensure the trustworthiness of staff operating the local SWIFT environment by performing personnel vetting.</td>
<td>n/a</td>
</tr>
<tr>
<td>5.4 Physical and Logical Password Storage</td>
<td>Protect physically and logically recorded passwords.</td>
<td>To ensure the security of passwords, Ekran System encrypts them and stores them in the Password Vault. Users can be authenticated on endpoints through Ekran System without credentials being revealed to users.</td>
</tr>
<tr>
<td>6. Detect Anomalous Activity to Systems or Transaction Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1 Malware Protection</td>
<td>Ensure that local SWIFT infrastructure is protected against malware.</td>
<td>n/a</td>
</tr>
<tr>
<td>6.2 Software Integrity</td>
<td>Ensure the software integrity of the SWIFT-related applications.</td>
<td>n/a</td>
</tr>
<tr>
<td>6.3 Database Integrity</td>
<td>Ensure the integrity of the database records for the SWIFT messaging interface.</td>
<td>n/a</td>
</tr>
</tbody>
</table>
### 6.4 Logging and Monitoring

Record security events and detect anomalous actions and operations within the local SWIFT environment.

Ekran System logs user sessions in a searchable video format, which is indexed with multilayer metadata. This metadata includes details such as application names, visited URLs, entered commands, the contents of started scripts, and keystrokes. Session details include remote IP addresses and host details. Session recordings can be exported for forensic examination.

Security staff can be alerted to a potential security breach using template-based and fully configurable alert rules, and log information can be forwarded to a SIEM system for more thorough analysis.

Changes in the Ekran System configuration are also logged. The system log is encrypted and protected by an anti-tampering mechanism.

<table>
<thead>
<tr>
<th>Security Control</th>
<th>Objective</th>
<th>Ekran System Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4 Logging and Monitoring</td>
<td>Record security events and detect anomalous actions and operations within</td>
<td>Ekran System logs user sessions in a searchable video format, which is indexed with multilayer metadata. This metadata includes details such as application names, visited URLs, entered commands, the contents of started scripts, and keystrokes. Session details include remote IP addresses and host details. Session recordings can be exported for forensic examination. Security staff can be alerted to a potential security breach using template-based and fully configurable alert rules, and log information can be forwarded to a SIEM system for more thorough analysis. Changes in the Ekran System configuration are also logged. The system log is encrypted and protected by an anti-tampering mechanism.</td>
</tr>
<tr>
<td>6.5A Intrusion Detection</td>
<td>Detect and prevent anomalous network activity into and within the local SWIFT environment.</td>
<td>n/a</td>
</tr>
</tbody>
</table>

### 7 Plan for Incident Response and Information Sharing

#### 7.1 Cyber Incident Response Planning

Ensure a consistent and effective approach for the management of cyber incidents.

To streamline cyber incident management, Ekran System provides a centralized UI for analyzing and reacting to detected incidents. Information about incidents can automatically be sent to a SIEM and/or a ticketing system.

To detect and prevent malicious or risky activity when detected, Ekran System provides incident response tools such as automatic and manual session termination, application termination, user warnings, and user blocking. To streamline incident management, Ekran System includes powerful reporting and investigation functionality.

<table>
<thead>
<tr>
<th>Security Control</th>
<th>Objective</th>
<th>Ekran System Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1 Cyber Incident Response Planning</td>
<td>Ensure a consistent and effective approach for the management of cyber incidents.</td>
<td>To streamline cyber incident management, Ekran System provides a centralized UI for analyzing and reacting to detected incidents. Information about incidents can automatically be sent to a SIEM and/or a ticketing system. To detect and prevent malicious or risky activity when detected, Ekran System provides incident response tools such as automatic and manual session termination, application termination, user warnings, and user blocking. To streamline incident management, Ekran System includes powerful reporting and investigation functionality.</td>
</tr>
<tr>
<td>7.2 Security Training and Awareness</td>
<td>Ensure all staff are aware of and fulfil their security responsibilities by performing regular security training and awareness activities.</td>
<td>n/a</td>
</tr>
<tr>
<td>7.3A Penetration Testing</td>
<td>Validate the operational security configuration and identify security gaps by performing penetration testing.</td>
<td>n/a</td>
</tr>
<tr>
<td>7.4A Scenario Risk Assessment</td>
<td>Evaluate the risk and readiness of the organisation based on plausible cyber attack scenarios.</td>
<td>n/a</td>
</tr>
</tbody>
</table>
DEPLOYMENT SCHEMES

Architecture Type A: SWIFT Infrastructure within a User Location

[Diagram showing the SWIFT infrastructure setup within a user location, including components such as SWIFT service provider, SWIFTNet, SWIFT secure zone, and general IT environment.]
DEPLOYMENT SCHEMES

Architecture Type B: SWIFT Infrastructure outside of a User Location
GET MORE DETAILS

Contact us

SWIFT sales:  swift@ekransystem.com
General inquiries:  info@ekransystem.com
Partner program:  partner@ekransystem.com

www.ekransystem.com

Ekran System®