CROSS DOMAIN SOLUTIONS

Secure System

SECURE SYSTEM OVERVIEW

A secure system starts with a solid architecture. link22 promotes building secure systems using standard components (COTS) rather than developing each system from scratch.

- Natural function growth as COTS mature
- Easier accreditation
- No need for costly in-house development
- Shorter time to go-live
- Use of supported components

LINK22 SECURE SYSTEM TEMPLATE

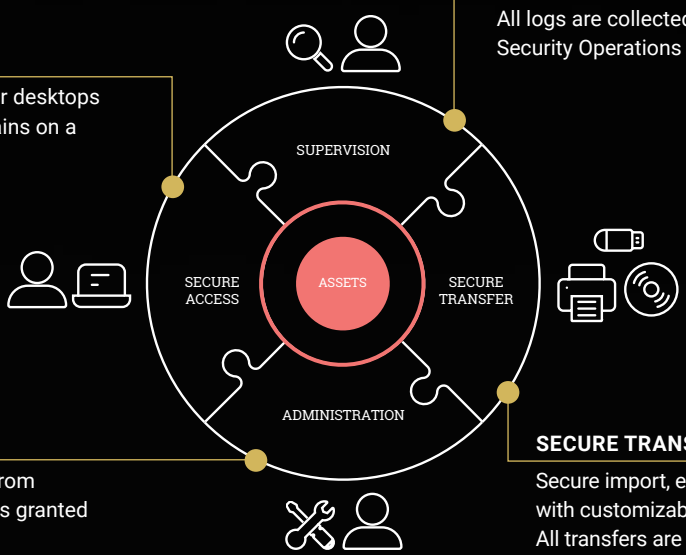
Most systems can can be seen as four interconnected parts that all are needed for a functional system.

SUPERVISION

All logs are collected and sent to a central Security Operations Center for log analysis.

SECURE ACCESS

Users are given access to user desktops in enclosed information domains on a need-to-know basis.



ADMINISTRATION

Administration is performed from hardened clients and access is granted based on role.

SECURE TRANSFER

Secure import, export and transfer of data with customizable content inspection. All transfers are strongly tied to users.

TEMPLATE REALIZATION

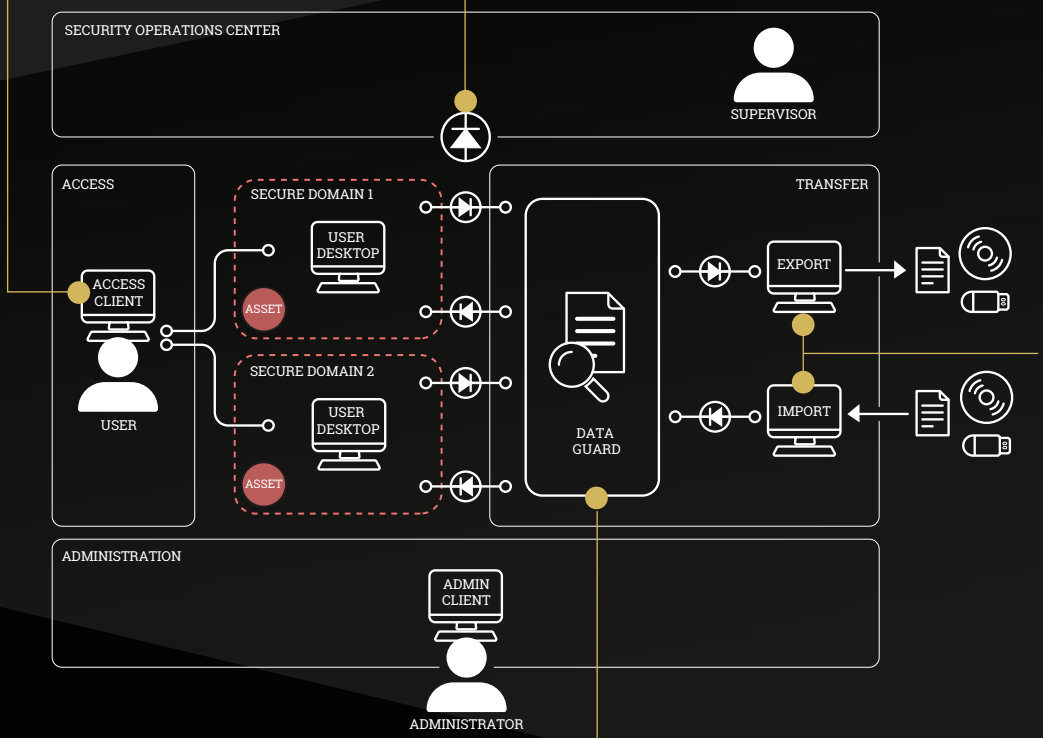
An actual system will be a tailoring of the system template taking the system's unique requirements into account. The simple example below shows a system with two separate information domains. Having multiple information domains is a simple way to enforce need-to-know separation within the same system.

ACCESS

Access to classified data from hardened clients.

LOG TRANSFER

Log transfer across data diodes prevents log manipulation and protects the system from the supervisors.



SECURE IMPORT AND EXPORT

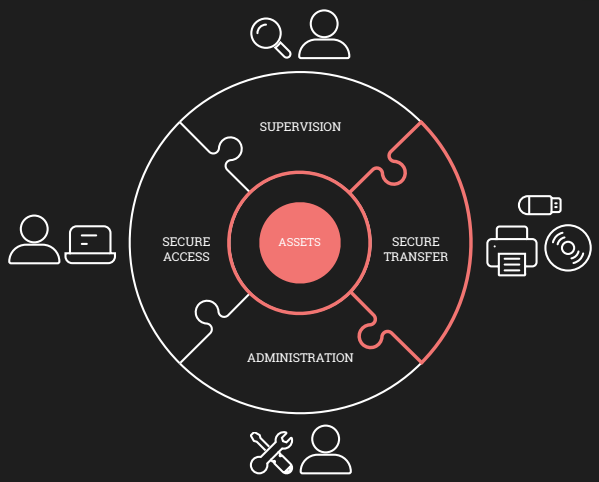
Kiosk applications allow secure import from and secure export to external media including printing and scanning.

DATA GUARD

All transfers pass the Data Guard that either approves or blocks transfer based on content and user identity.

SECURE TRANSFER OVERVIEW

Secure Transfer is a solution that enables transfer between isolated domains. All transfers pass a central Data Guard that performs content inspection and decides if the transfer is allowed.



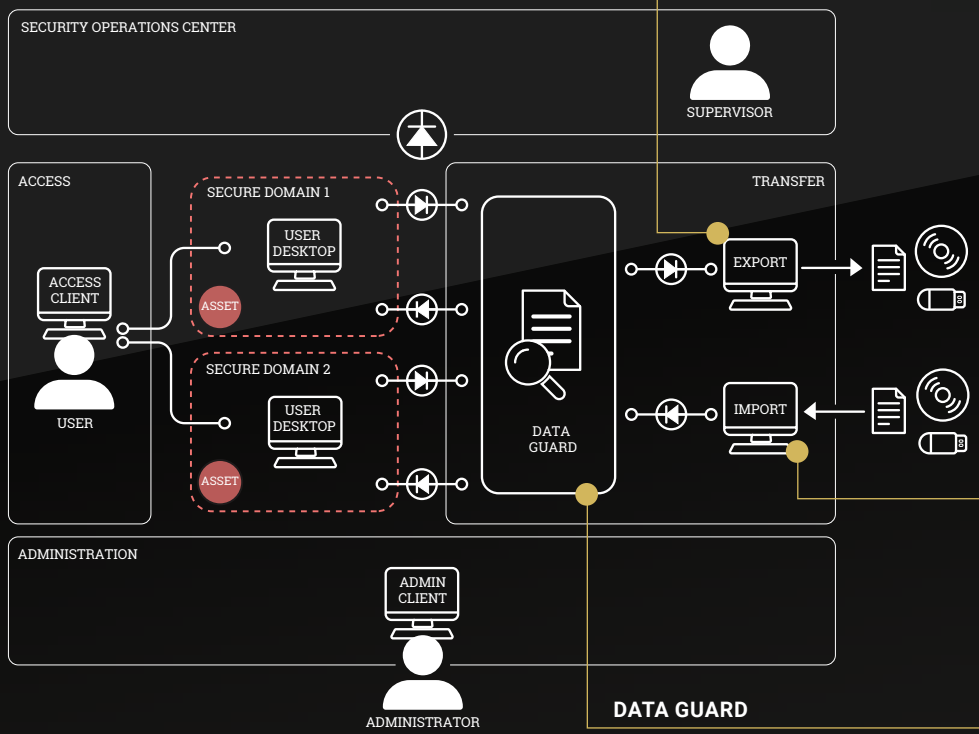
SECURE TRANSFER

MAIN BENEFITS

- Secure import to isolated environment
- Secure export from isolated environment
- Detection of malicious code
- All file transfers are strongly tied to user (non-repudiation)
- Customizable content inspection
- Works with any data diode
- Works with any smart card

SECURE EXPORT

Secure export is initiated by the user from the User Desktop where a local file is selected for export. The file is encrypted and encapsulated into a Secure Data Format before being sent to the Data Guard. Secure export to external media is done at the Export Station.



SECURE IMPORT

Secure import is performed from an Import Station where files can be imported from USB, CD/DVD and scanner. The imported files are encrypted and encapsulated in the Secure Data Format before being sent to the Data Guard. If the Data Guard approves the import the files are available from the User Desktop.

DATA GUARD

All transfers pass the Data Guard where they will be subject to content inspection, policy enforcement and authorization based on user´s smart card identity. Content inspection is fully customizable. Standard inspection filters are supplied and filter API can be used for custom filter development.

SECURE PRINT

Traditional printing solutions where the user sends their print jobs directly to the printers are vulnerable. The printer itself can be used to attack your IT-system since today's printers are known to be vulnerable to attacks. Also, with a traditional print solution the users are still at their workplace when the printing starts.

This can lead to loss of confidentiality and unnecessary printing. Our Secure Print handles these challenges by combining the benefits of traditional pull print with added security and strong authentication based on smart cards and unidirectional data flow using data diodes.

LEARN MORE

REASONS TO AIR-GAP NETWORKS

Air-gapping is achieved by separating two domains with a data diode. A data diode is a network equipment that on the physical level guarantees that data can only flow in one direction. A data diode provides a separation with much higher assurance than other mechanisms, such as firewalls.

The reasons for having air-gapped systems often fall into the following two categories:

ENSURE CONFIDENTIALITY

A closed system containing confidential information needs to be fed with information from an open systems while ensuring that no confidential information can leak to the open system.

EXAMPLES:

- Secure import of Operating System updates
- Supplying closed systems with time from an external NTP server

ENSURE INTEGRITY

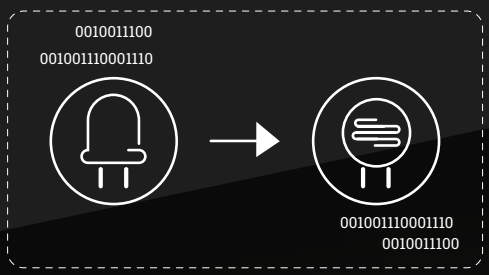
The secure system contains information that needs to be passed to an open system while ensuring that no modification of information in, or attack on, the secure system is possible.

EXAMPLES:

- Secure export of sensor readings in critical infrastructure systems
- Protection of data sent to log server

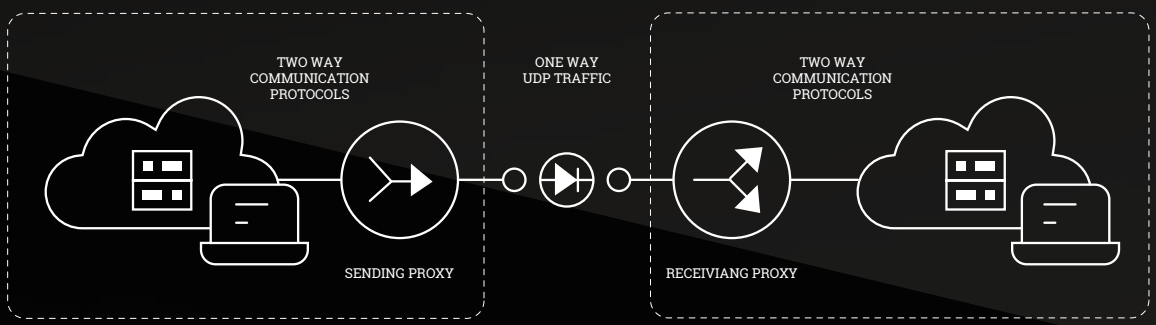
DATA DIODE

A data diode works by simple physics by sending light in one direction only to carry your data. A light emitter on one side sends light through a fibre to a photo receiver on the other end. Nature ensures that there is no way for the data to go in the other direction giving an unhackable air-gap bridge between networks. Firewalls and other software-based solutions will never be as secure. A firewall will always suffer from vulnerabilities and could be configured incorrectly.



DIODE PROXY

A data diode, in isolation, will only offer limited functionality unsuitable for most protocols, since support is limited to basic one-way UDP. Most systems will contain services that operate on a higher level, e.g. file, TCP or two-way UDP based. By adding proxy software hosted in either a virtual or physical computer on each side of the data diode, the more complex protocols can be supported. The proxy on the sending side converts the complex protocol to UDP for transfer over the diode and reconstruction in the receiving proxy.



CROSS-DOMAIN PRODUCTS

Read more about our products below. For the latest information and more details please visit diodetoolkit.com.

DIODE PROXY

Our product Diode Proxy is the cornerstone in Diode Toolkit offering reliable transfer including retransmission, bandwidth management, heartbeat functionality that detects link errors, integrity verification of transferred data ensuring that you can trust that the data has been transferred correctly and without errors.

The list of supported network protocols grows continuously and customers appreciate our powerful file transfer support. Diode Proxy is a software appliance based on Linux and runs on either physical or virtual hosts. Extensive hardening ensures secure integration in sensitive systems.

Diode Proxy is a proxy for data diodes and offers robust unidirectional communication across any data diode.

In addition to file transfer the following protocols are supported:

- UDP-streaming
- NTP
- Syslog

Diode Proxy will also offer:

- Flow control (bandwidth, retransmission etc.)
- Administration over HTTPS, SSH or local console
- SNMP supervision and heartbeat
- Delivered as a complete and hardened Linux installation

FILE TRANSFER

Diode Proxy offer robust and configurable file transfer.

The following protocols are supported:

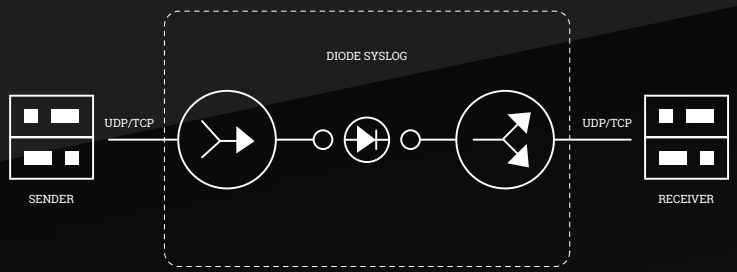
- CIFS / SMB
- NFS
- FTP
- SFTP

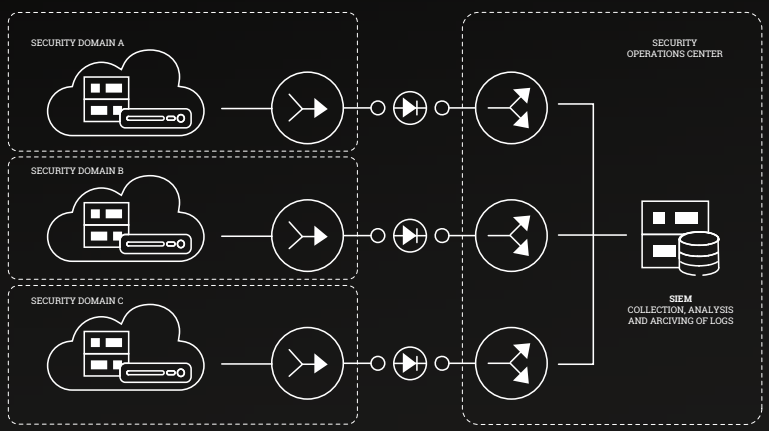
Diode Proxy can monitor a network folder shared either by the Diode Proxy or an external share from another server (Windows or Linux). Diode Proxy can be used for simple and direct file transfer (transfer mode) or to mirror a file structure (mirror mode).

DIODE SYSLOG

Diode Syslog can be configured to bridge the syslog protocol over data diodes. This setup allows many clients in the sending domain to send their syslog messages through a single point, the Upstream Proxy. Check out the Diode Syslog product if you are solely interested in the bridging of the syslog protocol.
It comes with a number of nice to have features and more complex syslog channel setups.

Diode Syslog provides support for transport of Syslog messages between two domains separated with a data diode. Both TCP and UDP protocols are supported and can be configured to run multiple parallel Syslog streams simultaneously. The most basic setup is to have a single Syslog stream as shown below.





MAIN FEATURES

- Diode Syslog is able to forward Syslog messages from multiple computers to multiple Syslog servers in a different network separated by a data diode
- Diode Syslog is able to redirect Syslog messages to different Syslog servers depending on which port Diode Syslog received them
- The downstream proxy is able to detect malfunction of both the upstream proxy and/or the data diode
- Diode Syslog is able to cache Syslog messages if the data diode is malfunctioning or if the connection to the destination Syslog server is broken

DATA DIODE ZERO

Our Data Diode Zero is a small and affordable network component that allows network traffic in one direction only. It can be used to ensure confidentiality or integrity, it depends on how you use it.

MAIN FEATURES

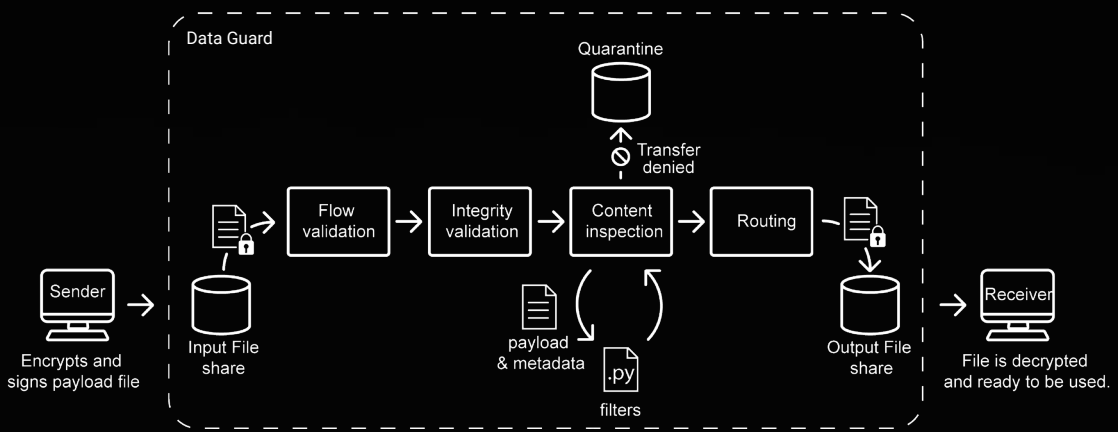
- More secure separation than using a firewall
- 1 Gbit/s throughput
- Ethernet Interface
- Built in optical separation

DATA GUARD

The central part of Secure Transfer is the Data Guard that performs:

- Content inspection
- Transfer routing based on cryptographic metadata
- PKI-aware authorization of transfers
- Configuration of transfer routes

All imports and exports pass through the Data Guard that decides if the transfer is allowed based on transfer metadata and contents of transferred data.



CONTENT INSPECTION

All transfer flows pass the Data Guard and all files will be subject to content inspection. The transfer is allowed or blocked based on configuration and the transferred file. Content inspection is performed on the actual payload and not the encrypted transfer.

The content inspection is done by fully customizable filters. Several standard filters are supplied, e.g. for anti virus scanning and black/white listing based on file MIME-type. A filter API allows for development of filters that can implement any policy decision.

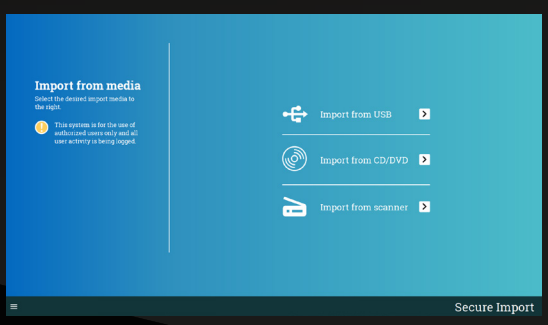
A transfer that is blocked by content inspection will be quarantined and the receiver will be notified. A Secure Transfer administrator may override the content inspection and resume the transfer if an investigation shows that the block was unintentional.

DEEP INSPECTION

Content Disarm and Reconstruction (CDR) functionality can be added as an additional Data Guard inspection module. This feature sanitizes and rebuilds each file to ensure a safe an clean content. The CDR functionality is an option in the Data Guard.

SECURE IMPORT CLIENT

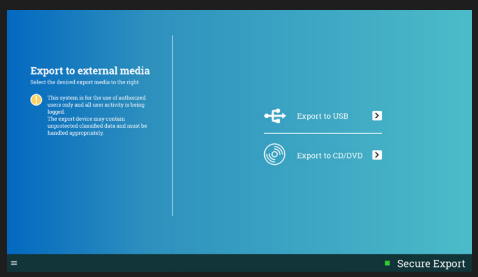
Adds the possibility to securely import data from digital media into a secure system. The Secure Import Client typically runs in Kiosk mode at the system border. The import is tied to the importing user by cryptographic means ensuring full accountability.



- Windows Kiosk application
- Import files from:
  - USB storage device
  - CD/DVD
  - Scanner
- Supports multiple destinations
- Smart card aware

SECURE EXPORT CLIENT

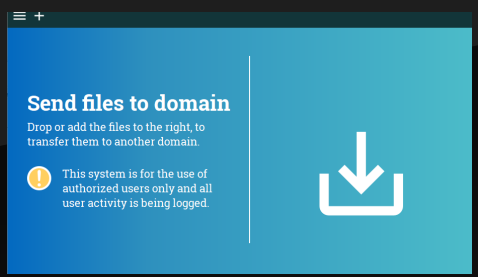
Adds the possibility to securely export data to digital media from within a secure IT-system. The Secure Export Client typically runs in Kiosk mode and is placed at the system border.



- Windows Kiosk application
- Export files to:
  - USB storage device
  - CD/DVD
  - Smart card aware

SECURE TRANSFER CLIENT

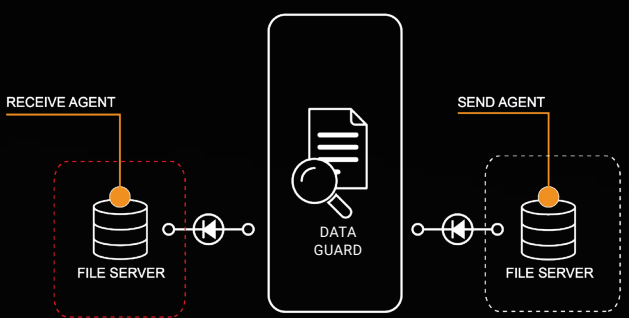
A software enabling a user to send and receive files from a User Desktop inside a Secure IT-system. It is an integral part of the Secure Transfer solution and has full support for content inspection and policy enforcement.



- Windows application
- Separate applications for sending and receiving files
- Smart card aware

SECURE TRANSFER AGENT

Secure Transfer Agent consists of software that is installed as a service that is configured to monitor local directories. Is designed to automatically send files between security domains whose boundaries are protected by data diodes.



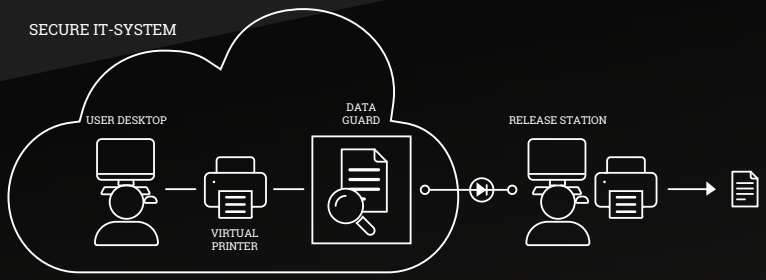
- Agent-based solution that can monitor directories in real time.
- Use soft certificates to encrypt flows
- Easy to integrate with link22 Data Guard

SECURE PRINT

It is simple to print from the user's Windows desktop in the Secure IT-system as Secure Print appears as a standard printer allowing printing from any print capable application. The printout is encapsulated into a file and encrypted and signed using the user's smart card before it is forwarded. Secure Print is compatible with link22 Data Guard allowing for policy enforcement of printing. Once passed the Data Guard the print job is available for printout from any Release Station after smart card login.

The print job is decrypted only when selected for printing and is directly printed to the physical printer attached to the Release Station.

- Printer independent
- Simple client administration
- Pull print



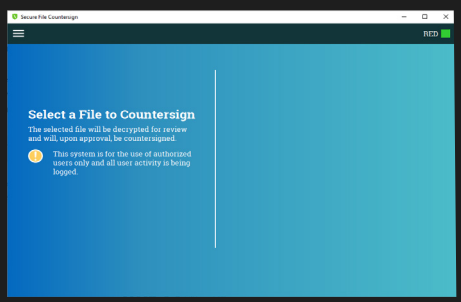
MAIN FEATURES

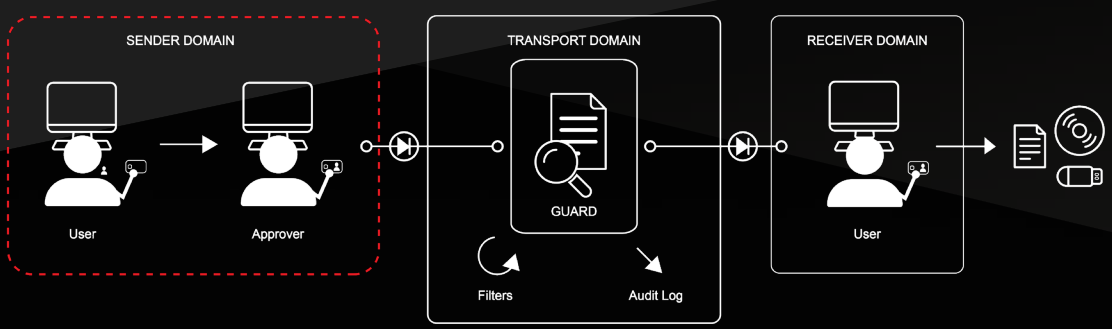
- Users pick a printer as they walk, not from their client
- Every print job is signed and encrypted with the user desktop
- Simple administration, From within you IT System the user is presented with a single virtual printer

SECURE FILE COUNTERSIGN

Secure File Countersign is a software module designed to perform counter signatures. An inspector whose function is to grant or deny files passing over an interface uses this application. The inspector in question uses this application to review and verify that a file is approved for export. Accepted files are granted with a signature (countersignature) created using the controlling party's smart card. The file can then continue to the next step in the chain where the link22 Data Guard verifies that the file has been countersigned by an approved controller.

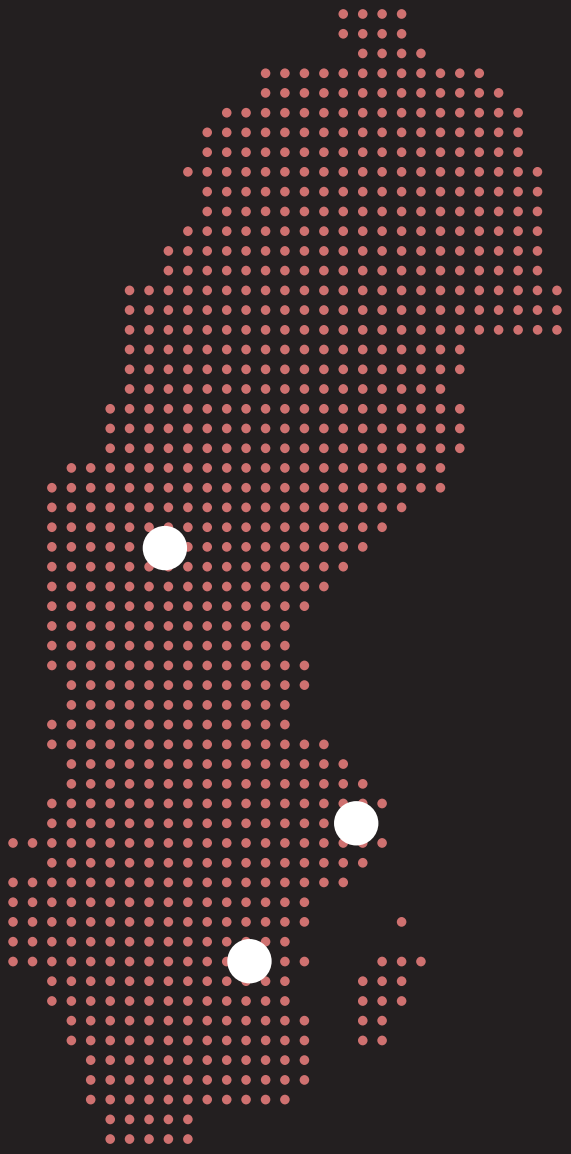
- Smart card aware
- Easy to integrate with link22 Data Guard
- Designed for Export control





MAIN FEATURES

- Developed graphical interface with user-friendliness in focus.
- Can be easily integrated with link22 Data Guard to verify that a file has been countersigned, according to configurable rules.
- Files are protected with a transport protection connected to the user's smart card.
- Configured with windows Active Directory and group policy.



Head office Linköping

link22 AB
Teknikringen 8
583 30 Linköping
Sweden

Phone +46 13 13 24 00
info@link22.se

Östersund

link22 AB
Kyrkgatan 53
831 34 Östersund

Stockholm

link22 AB
Tellusvägen 43
186 36 Vallentuna