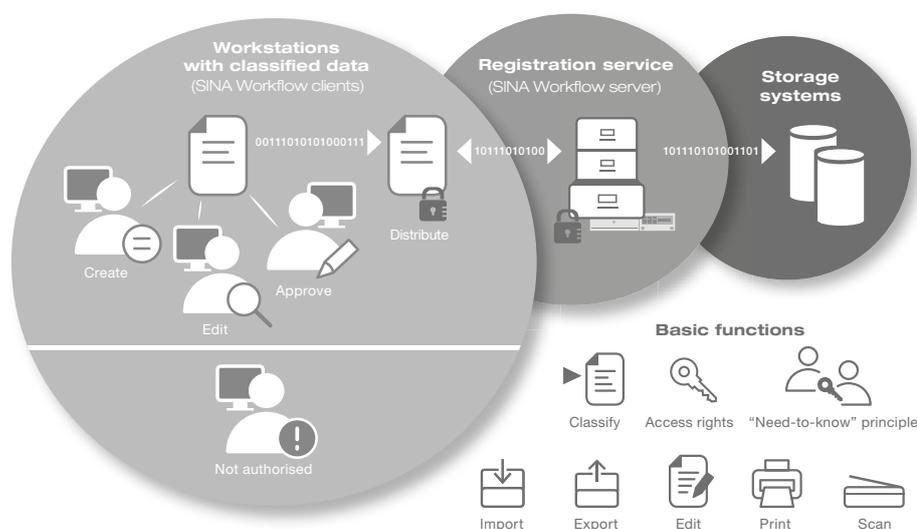


## Secure Workflow System for Classified Information (CI)

### SINA Workflow Compliant to security rules for CI



### Benefits:

- » Compliance with security rules for CI
- » Enforcement of the "need to know" principle
- » Administration of CI documents in files and processes
- » CI importing and exporting
- » Revision-proof verification
- » Runs on current SINA Workstations
- » Under evaluation for German national GEHEIM

The SINA Workflow system solution guarantees secure, thorough and compliant implementation of individual business processes involving classified information and other valuable documents. SINA Workflow comes into effect when drafts are being drawn up, protecting data throughout the entire lifetime to destruction. This modular system solution also supports the import and export of classified data and is prepared for exchanging classified data across all domains.

#### Initial situation and motivation

It was not previously possible to process electronic classified documents without media discontinuity. IT-supported classified registries only addressed the traditional, paper-based classified document world. This meant that, while it was possible to create classified documents by electronic means, it was only possible to collect them in the form of print-outs because there were no approved electronic classified registries. In addition, there was a lack of a consistent cryptographically supported implementation of the "need to know" principle in classified information processing. Until now, the market has not offered any solutions that meet the requirements of the security rules for classified information. This means, for example, that approval and co-signatory processes (workflows) are almost all implemented through organisational measures. With SINA Workflow, there is now a reliable, thorough cryptographic solution for the first time.

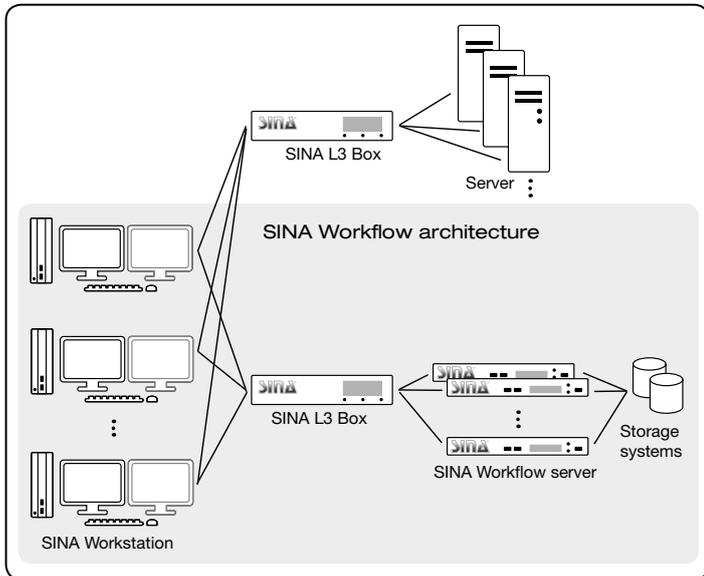
#### What does conformity with security rules for classified information mean?

One of the most important features of any electronic CI registry is functional conformity with existing provisions (for example the German Federal Ministry of the Interior's security rules for classified information). This forms the basis for using corresponding CI registries in authorities as standard and adhering to the defined basic principles. These basic principles specifically include provisions on identifying, marking, distributing, copying, storing, archiving and destroying classified information.

SINA Workflow is flexible enough to support even the provisions of other public agency sectors or nations. Examples of this are requirements pertaining to the administration of official written materials, the Common Ministerial Rules of Procedure (German regulations) or police directives.

**Components and functionality**

SINA Workflow is a system network of secure SINA Workstations and scalable SINA Workflow servers, with an integrated CI registry and central network storage.



SINA Workstations are secure workstations in the SINA Workflow architecture and are used and configured accordingly. Besides functions for creating and processing classified information in integrated working environments (sessions), these clients have additional SINA Workflow client-based functions for interacting with an CI registry. The SINA Workflow client provides all the processing functions for classified documents, including:

- Registration (including version management)
- Classified information process management
- Distribution according to the “need to know” principle
- Deployment on a “need to share” basis
- Importing and exporting
- Printing

In addition, every data exchange between the workstations and central components is secured using SINA technology.

The **SINA Workflow Server** in the network provides an electronic CI registry and workflow services. The latter includes user management, workflow management, classified information administration, classified information inventory, system administration and verification. SINA Workflow servers can be easily integrated into any popular network management system.

Classified documents exchanged via a SINA Workflow Server are encrypted and decrypted in the SINA Workflow client for implementing the “need to know” principle. In addition these classified documents have an integrated **labelling function** and are cryptographically allocated a security label and metadata (including confidentiality classification, creator and keywords).

**How the architecture functions**

SINA Workflow allocates various roles (for example classified information processor, the recipient, the administrator and the security officer), which are associated with rights within the network. A coordinated working method for those involved is made possible in the context of pre-configured workflows via the SINA Workflow client graphic user interface. This includes exchanging information on the status and progress of the relevant workflow and the allocation or placement of tasks.

The system also supports decisions relating to classified information, including such things as the allocation and acceptance of access rights and approval of the distribution of classified information.

**Integration in application environments**

secunet can help you by offering advice on all aspects of the integration of SINA Workflow systems. Starting with the classified information core reference processes, there is an initial status review of existing application environments, including analysis of the relevant user roles and the classified information processes implemented.

The requirements for integration into the existing IT systems are derived from this status quo. The relevant interfaces and data exchange procedures for this are identified and prepared.

The actual installation/integration then takes place and the required SINA Workflow users are set up, including preparation of the associated cryptographic keys and certificates on SINA Workflow smart cards.

After the integration is concluded, the classified data already on the system is imported into the SINA Workflow system as required, labelled and made available as core classified data stock.

The SINA Workflow system also supports the incorporation of existing classified or open databases.

**Network components**

Components	SINA Software
SINA Workstation E or H	Version 2.6 or higher with virtualised SINA Workflow client
SINA Workflow Server Appliance(s)	Virtualised guest operating system: Debian 6.0 Host operating system: Ubuntu 12.04

More information:  
[www.secunet.com/en/sina](http://www.secunet.com/en/sina)

**secunet** secunet Security Networks AG  
 Phone: +49 - 201 - 54 54 - 0  
 Fax: +49 - 201 - 54 54 - 1000  
 E-mail: [info@secunet.com](mailto:info@secunet.com)  
[www.secunet.com](http://www.secunet.com)