



# SE46 Application Whitelisting

## Total protection against IT security threats

Cryptzone's SE46 Application Whitelisting solution ensures that only trusted software and hardware is allowed to run on mission-critical machines and computer workstations.

Using the principle of "Deny by Default" SE46 treats any file that is not part of an authorized application as

undesirable and never permits it to start. The result is that any virus or unauthorized software is completely blocked and therefore can never pose a threat.

SE46 Application Whitelisting can protect any type of Microsoft Windows® based device or system: for example industrial robots, process control and surveillance systems, traditional office PC's and servers, ATM machines, medical equipment, military and retail EPOS systems.

## SE46 – Three Components

### SE46 Desktop or Server Agent

The SE46 Agent is the software agent installed on all systems that SE46 must protect. Once installed the Agent intercepts all attempts to execute software. At the point any software attempts to run it is compared with the list of approved applications that have been assigned an Application Certificate.

Application Certificates are electronic ID-cards created and assigned to software programs. Just like an electronic ID (eID) can identify a person, an Application Certificate uses the same principle to identify a specific program and all its components. If no match is found the program is prevented from starting. The SE46 Agent is a completely stand alone system.

It requires no contact with the SE46 Lookup and Logging Server to maintain a high level of security. Therefore it is ideal for use within environments where there is no network connectivity.

SE46 can protect any type of Microsoft Windows based device or system

### SE46 Lookup and Logging Server (LLS)

LLS is mainly used for the storage and distribution of Application and Policy Certificates. In addition to collecting log data from SE46 Agents, the LLS is where functions such as "Application Reverse Lookup" and reporting are initiated. SE46 reports show where and when software is running on secured systems.

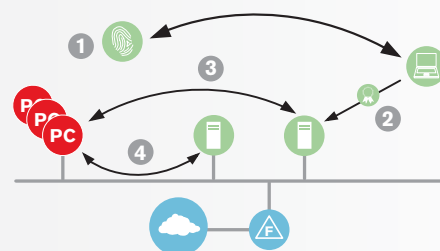
### SE46 Certificate Studio (CS)

CS is the operator program that is used to create Application & Policy Certificates.

SE46 CS is an advanced tool for analyzing and categorizing which components are part of which trusted applications. SE46 CS is also used to create the policy rules that SE46 Agents should enforce on the security targets.

### 4 Steps, 5 minutes:

1. Collect the fingerprints
2. Create and publish Application Certificates
3. Distribution of Application Certificates
4. Reporting log data



# SE46 Features

## Anti-Virus

SE46 provides proactive protection against:

- Intrusions attacks
- Known and unknown viruses, Trojans and other threats
- Spyware, malware and ad-ware
- Untrusted scripts

## Quality improvement

- Inventory audit – discover all executable software on your computers
- Full version control of in-house as well as third party tools and applications
- Traceability of when applications are introduced, used or removed

## License management

- Eases license management
- Produces accurate reports of exactly what, where, when and how long applications are running within your organization

## Version Management

- Control over which software versions are installed
- Prevent the “wrong” software versions from running
- Force users to upgrade to the correct version
- Clean out older versions

## Log Management

- Centralized logging and certificate storage
- Application fingerprint verification in real time

## ITIL

- Truly proactive
- Time limited certificates with expiration dates provide business flexibility
- Users cannot be distracted by non approved applications
- Known and unknown Trojans, spyware and viruses are stopped simply and effectively
- Easy process-oriented administration via digitally signed policies
- Fewer incidents for the Service Desk.

- No change without change control
- 100% adaptable for SLA down to an application level

## Central control

- Application & Policy Certificates are created using the Certificate Studio
- The operator creates the Application Certificates centrally and distributes them to all other computers

## Cleanup/Removal

- The “Xile” function makes sure hard drives are purged of all undesirable software

## Stand Alone

- Every SE46 (agent) knows where to look for its updates
- All pull and no push technolog

## Policy based

- Only the approved configuration is permitted
- Time limitations and expiration dates
- Central distribution with unique distribution point for each policy
- Central control over users and their application rights
- Electronic ID-cards
- Applications Certificates are electronic
- IDs for computer programs
- Application Certificates identify all executable software
- Policies trust one or more issuers of IDs
- Deny certificate to block undesirable applications

## Active Directory

- If preferred third party tools, such as Microsoft™ Active Directory can be used to distribute Application & Policy Certificates.

## Hardware control

- USB adapters cannot connect without approval
- PC cards must have valid application certificates
- Every hardware device that connects must be a trusted device



**Microsoft Partner**

Gold Independent Software Vendor (ISV)

Cryptzone solutions mitigate information security risks in the key areas of Policy Compliance, Content Security, Secure Access and Endpoint Security.

### International Headquarters

Cryptzone Group AB  
Drakegatan 7,  
SE-412 50 Gothenburg,  
Sweden

[www.cryptzone.com](http://www.cryptzone.com)  
[info@cryptzone.com](mailto:info@cryptzone.com)

### Regional Offices

Sweden  
Tel: +46 (0)31 773 86 00

United States  
Tel: +1.949.279.6177

United Kingdom  
Tel: +44 (0)370 013 1600

### Partner information:

For more information go to  
[www.cryptzone.com/partners](http://www.cryptzone.com/partners)