CODESEALER
INVISIBLE END-TO-END WEB SECURITY

August 2016

White Paper

INVISIBLE END-TO-END WEB SECURITY

CYBERCRIME, A GROWING THREAT

THE INCREASING CHALLENGE OF CYBER CRIME

Cybercrime, is spreading at an alarming rate. It has today become a global multi-billion-dollar criminal operation. Every day cybercriminals develop new and more complex online attacks. Corporates and the public sector face loss of data, money and customer credibility and each year companies spend large amounts protecting their transactions.

YOUR CUSTOMER IS THE MAIN TARGET

Unfortunately, customers' devices are often the target, computers are infected, sessions are hijacked and malicious attacks occur. Many products rely on installation of dedicated security programs and companies relying on their customers' willingness and/or ability to take the necessary security measures. Downloads and installations can be complex, users may not have the appropriate administration rights, and the vulnerability against attacks is therefore a serious threat. With approximately 75% of all computers infected, it may seem impossible to protect the customer and your company against malicious attacks. Security solutions and organizations alike are challenged by the constant introduction of new attacks, and keeping security software up to date is an significant part of todays IT costs.

PROTECTING AGAINST MALICIOUS ATTACKS

Is it possible to protect and secure online sessions on an insecure platform?

Can sessions and browsers be protected, even if the device is infected?

The answer is yes.

CodeSealer's solution applies unique client code obfuscation for each session, added encryption of all communication and encapsulation of the browser sessions.

While no solution can protect 100%, obfuscated and sealed sessions will dramatically improve the security, and cybercriminals will constantly be faced with changed and hidden application code making it virtually impossible to re-use malicious attacks.

The results of this approach is that a secure session between the customers' browser and the online system can be established. It can be used to continuously monitor the web page displayed to the user and react to unknown and malicious changes.

"Cybercrime is a growing industry.

The returns are great, and the risks are low. We estimate that the likely annual cost to the global economy from cybercrime is more than $**445** billion, including both the gains to criminals and the costs to companies for recovery and defense.

A conservative estimate would be $**375** billion in losses, while the maximum could be as much as $**575** billion."

The cyber crime hitlist
20 cyber crime cases under probe
Keeping Your Bank Account Safe on the Internet
High-tech war on cybercrime
Hacking Britai
Cyber crime costs UK up to £27bn a year
Mail Online
Science & Tech
Cyber Crime Victims Have Nowhere to Go
New PC virus doesn't just steal your money - it creates fake online bank statements so you even don't know it's gone

Source: Intel Security
Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II
Center for Strategic and International Studies   June 2014

WSF

CodeSealer offers a next-generation solution to protect websites against malicious attacks with its main product WSF. While traditional Web Application Firewalls protect the web server against known attacks, WSF encapsulates and protects the entire website, including web server, web browser and the communication between them. In this way, any organization can let its customers conduct trusted online transactions even from a compromised device and over an insecure network.

Statistics confirm that more than 75% of all devices today are infected. WSF will not only protect your website but also your customer - despite infections. Compared to other security products, WSF does not need to know the attack type beforehand, nor does it search for known attacks on the customer's device. WSF is offering a truly unique end-to-end web session security without customer installations, instantly covering all of your customers.

WSF is completely invisible to your customers, providing a significant added value compared to other security products. WSF is installed as a protection in front of your web server and handles all communication between the web server and the customers' device at web browser level. This is security one step further than any other product. The enhanced encryption, hidden application code, obfuscation, and key exchange provide security beyond what has been possible until today.

WSF — HIGHLIGHTS

- **A single, invisible, server based product protecting web sessions and data transmissions**
- **Even protects against unknown malware and attacks**
- **Control, monitors and protects web pages, by monitoring all activity at browser level**
- **Protects web traffic by use of additional encryption, dynamic obfuscation and session keys**
- **No customer installation required and therefore 100% instant coverage**
- **Ability to abort all malicious sessions and attacks**
- **Provides forensic reports**

PROTECTION

CodeSealer’s WSF provides a unique protection against man-in-the-browser and man-in-the-middle attacks, not matched by any other product. Where many products protect against known malicious attacks, WSF even protects against unknown attacks, using our patented technology.

WEB INJECTION ATTACKS

Unprotected websites are open for malicious attacks, and web injection tools can be installed in the browser and/or operating system. This is done in such a way that all data sent between the web server and the browser is accessible (read and write) in non-encrypted form. The malicious software operates after HTTPS encryption has been opened, and HTTPS does not prevent web inject attacks.

WSF adds an extra layer of encryption at browser level, providing security one step further than HTTPS. WSF ensures that the traffic passing a potential web injection is encrypted and authenticated. While no 100% solution exists today, the extra layer of security makes an attempt a long and tedious process and the attacker may instead attack less secured sites.

DOM MANIPULATION / INJECTIONS ATTACKS (BROWSER PLUGIN)

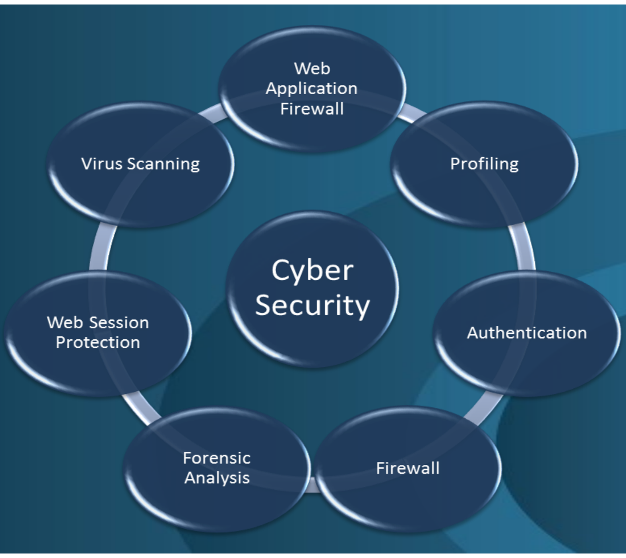
If a malicious browser plugin or browser helper object has been installed in the customer’s browser, it can access the full content of any web page visited by the customer.

WSF continuously monitors the protected web page while displayed in the customer’s browser and detect any attempts to make unauthorized changes to the protected web page. The extra layer of our patented technology safeguards your pages.

SESSION / COOKIE HIJACKING

Today attackers install malicious tools that can read the network traffic, steal the session cookie, and impersonate the victim. Other attacks obtain the session cookie from the memory contents of the customer’s computer, opening it up for fraud and misuse of data.

WSF encryption ensures all the way into the WSF client running in the browser, making HTTP inspection impossible. The WSF Client protects session cookies, and the attacker is left with a secure session and a failed attempt of hijacking.

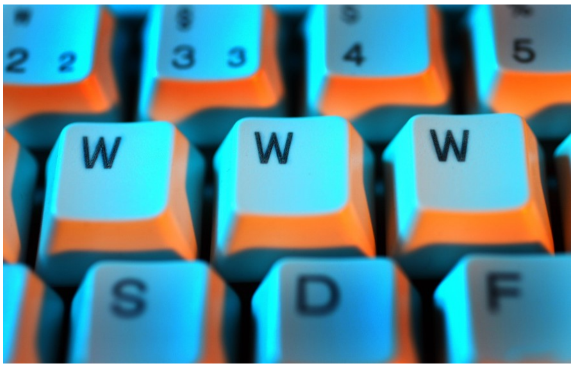


WSF PROVIDES A UNIQUE ADDITION TO A COMPLETE SOLUTION

FEATURES

CodeSealer's WSF offers unique protection, adding to the already built-in and implemented layers of HTTPS and complimentary products.

INSTANT COVERAGE, NO CUSTOMER INSTALLATION



Today customers access your web pages from multiple sites, e.g. at home, the office or from public devices. While many products today require your customer to download and install security on their devices, WSF provides instant security for all your customers as soon as it has been installed within your environment.

BUILT-IN BOOTLOADER

The built-in Bootloader protects the session, using dedicated session keys, dynamic obfuscation and additional encryption.

OBFUSCATION

All sessions are protected by unique obfuscation of data. The dynamic obfuscation hides code patterns, statements and functions, leaving an attackers without traces and insight. All in a manner in which they will not have sufficient time to break the code.

ENCRYPTION

While HTTPS encryption provides security between the HTTPS gateway, on the server-side infrastructure to the SSL/TLS termination point in the browser, WSF goes one step further.

Installing WSF adds an extra layer of encryption and authentication inside the HTTPS layer. The WSF encryption protects from the WSF server, on the server-side infrastructure, to the WSF client running in the customer's browser.

In addition, WSF encrypts all URL on the website preventing SQL injection and Cross-Site Scripting through URL parameters, hiding not only the URL but also the server-side structure of the website.

Increased Security

Invisible

Session Handling

Customizable

Web Page Protection

100% Coverage

FEATURES

- Invisible and no customer installation required
- 100% instant coverage
- Increased security encapsulation and monitoring of the Web Session and Browser , even protecting against unknown malware and attacks
- Additional encryption and protection of session, beyond SSL/HTTPS
- Authentication of session, using unique keys
- Obfuscated handling of session through a dynamic Bootloader
- Customization of malicious attacks handling

FEATURES, continued

CodeSealer's WSF offers more than just session protection, it also secures your web pages and their content.

HIDDEN APPLICATION CODE

WSF stores and executes all of the web-site's JavaScript code inside the WSF client, making it virtually impossible to access. Identifying and analyzing code will become a tedious process, preventing attacks of the web-site's JavaScript code.

WEB PAGE ENCAPSULATION AND MONITORING (Web Shield)

Where most security solutions today protect against known, malicious attacks, WSF goes one step further. WSF will not look for known attacks. By encapsulating the web session, WSF ensures that web pages are not manipulated, pages are displayed as intended and data entered sent as entered. WSF constantly monitors and reacts to any change by comparing the result with the page received by the WSF server.

FORENSIC REPORTING AND HANDLING

Should web pages or sessions be attacked, it does not only have the advantage of increased security. WSF can be configured to handle malicious attacks in multiple ways:

- Notifying IT Service Management while keeping the session alive and allow the customer to continue
- Redirecting the customer to a specific web-page, such as a validation page or log-in
- Terminating the session and returning the customer to the start page
- Providing forensic report and data for security analysis

CUSTOMIZABLE

WSF adds a unique layer of security. Infrastructure varies from company to company and WSF has been built to support your existing infrastructure. Domains and individual pages can be turned on and off, features controlled, utilization can be managed and the range of platforms supported is flexible.

WSF Server:
- Deployment within existing infrastructure
- Acts as HTTP client towards protected web server
- Handling of WSF Client and sessions

WSF Client
- JavaScript solution automatically inserted into the web site by WSF Server

Protection:
- Server side, ensuring only authenticated access
- Encryption of HTML, JavaScript, CSS and AJAX data transmitted and stored in browser cache
- JavaScript and session cookies stored and executed in protected environment
- Detection of unauthorized modifications to web pages
- Cryptographic support, such as Rabbit Stream Cipher, Badger Message Authentication Algorithm, SHA

FEATURES, continued

CodeSealer’s WSF provides easy deployment and support setup, making it a safe and complimentary product to your existing platform and security.

BROWSERS

All browsers’ can be utilized using WSF, and all common browsers in supported versions are protected by the unique WSF security. The following browsers are protected by the full level of security:

- Internet Explorer 9+
- Google Chrome/Chromium
- Mozilla Firefox
- Safari
- Opera

MOBILE SOLUTIONS

Not only does WSF protect desktops, it also protects web browsers across mobile devices.

Browsers and Web View Apps, used on a mobile device, are protected with the same high level of security, without further installation or development. Covering these, WSF provides security for the majority of all mobile Apps, and your complete platform is secured as Native Apps are often built with a built-in security.

SETUP

Deployment of WSF is done within your own secured network, behind DMZ and Firewall, and the WSF Server supports standards such as Linux, Solaris, AIX and Windows Server.

PLATFORMS AND DEVICES

WSF can be installed on common operating systems used for hosting web sites, such as Red Hat Enterprise, Debian based Linux distributions, Windows Server, Solaris and AIX.

Furthermore, WSF supports all common browsers across devices

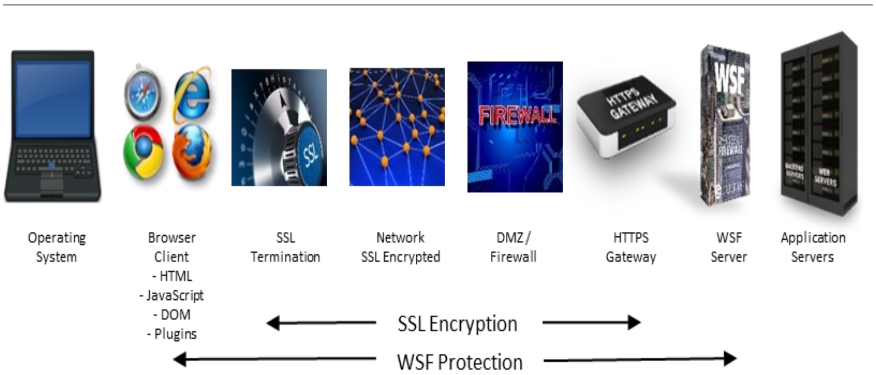
- Internet Explorer 9+
- Google Chrome/Chromium
- Mozilla Firefox
- Safari
- Opera

Web Session Firewall Supports HTML 4, EcmaScript 3+ and some HTML 5

WSF—OVERVIEW

DEPLOYMENT

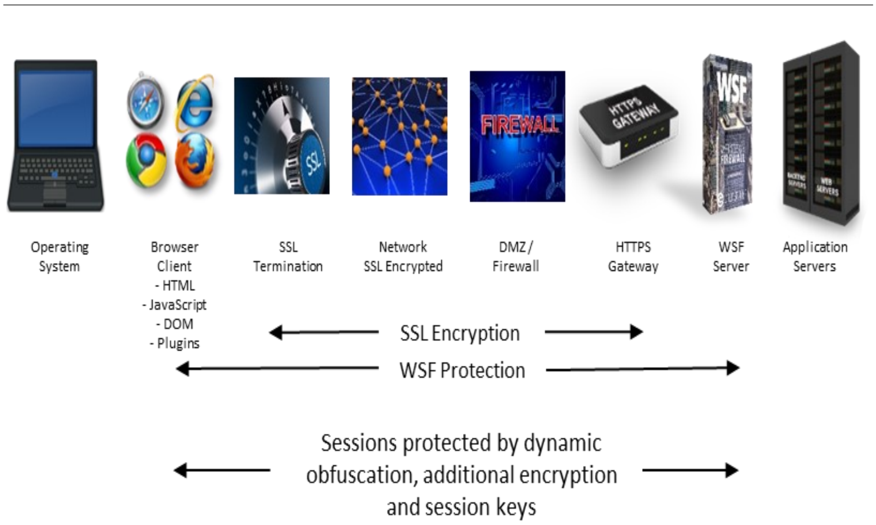
WSF Deployment



WSF is installed within an existing infrastructure, in front of the web server hosting the web sites, but behind HTTPS gateways and load balancers. Once installed, it will automatically ensure that the WSF client component is started for all web sessions. The WSF client is protected by the built in WSF Bootloader, ensuring that the WSF client is safe, has not been tampered with, and has a secure communication to the WSF server.

SESSION ESTABLISHMENT

WSF Session Establishment

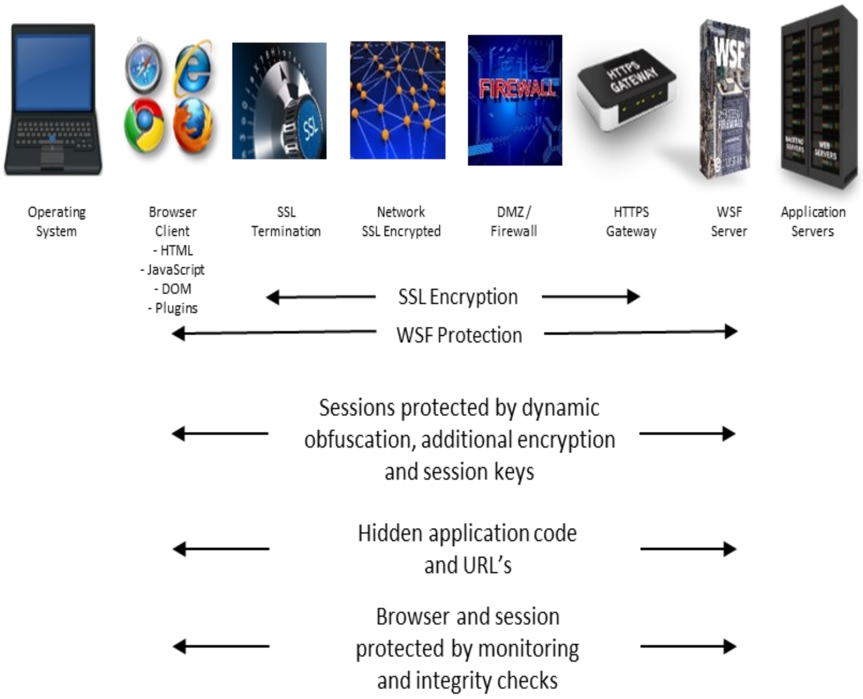


When a customer enters a protected web site, through a valid URL, following a link or a bookmark the first session is initiated. The WSF server responds to the web browser and an invisible WSF client is initiated within the browser, without customer interaction. While HTTPS encrypt the session at SSL/TLS termination point, WSF not only adds an extra layer of encryption, it also goes one step further and protects the browser and terminates in the WSF client. The WSF client establishes a secure session and exchange cryptographic keys for encryption and authentication of all subsequent communication.

WSF—OVERVIEW, continued

DISPLAYING A WEB PAGE

WSF Displaying a Web Page


Operating System
Browser Client - HTML - JavaScript - DOM - Plugins
SSL Termination
Network SSL Encrypted
DMZ / Firewall
HTTPS Gateway
WSF Server
Application Servers
SSL Encryption
WSF Protection
Sessions protected by dynamic obfuscation, additional encryption and session keys
Hidden application code and URL's
Browser and session protected by monitoring and integrity checks

Using the secured session, WSF client sends a request to the WSF server for the initial web page requested by the customer. The WSF server validates the request and communicates with the web server. The reply from the web server is encrypted by the WSF server and sent to the WSF client in encrypted form. The WSF client verifies the response, decrypts, decompresses and divides the response into a visible and invisible content. The visible (HTML code, style sheets, images, etc.) is sent to the browser's rendering engine and displayed to the customer. The invisible part (JavaScript code, cookies, etc.) is stored securely within the WSF client. The displayed web page is monitored at browser level in order to detect potential malicious attacks. Customer entries are monitored to ensure that they are forwarded as entered.

WEB PAGE INTEGRITY CHECK

In addition to additional encryption, obfuscation and session key handling, the main feature of WSF is to encapsulate, monitor and prevent manipulation. The WSF client will forward requests to the WSF server, including a list of potential issues. The WSF server validates the encrypted and authenticated session and compares the received with the initial web page sent to the customer. Only allowed changes, such as input forms, will be allowed and passed on to the protected web server. All other changes will be identified as potential illegal changes. Based on customized parameters the WSF server can redirect the malicious input to an error page or simply disconnect the customer.

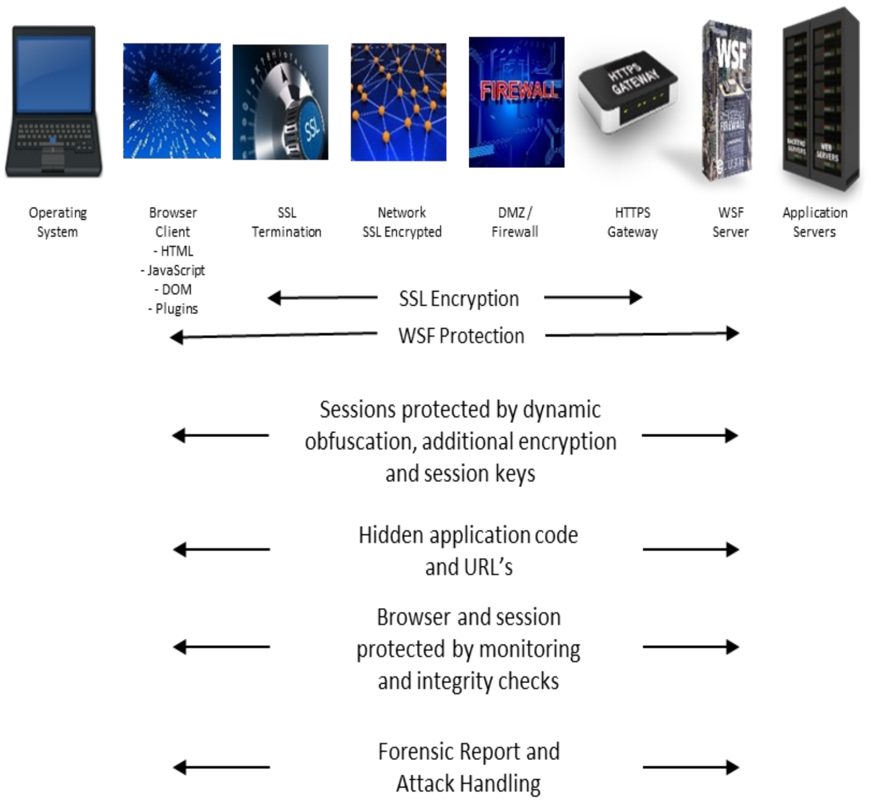
WSF—OVERVIEW, continued

ATTACKS

Web Injection Attacks: Inject tools are installed after the termination of HTTPS, and all data are vulnerable for theft and manipulation. WSF protects one step further and WSF will not only add an extra layer of encryption, it will provide termination within the WSF client, leaving the attacker with useless information.

Browser Plugin: Malicious browser plugins or browser helper objects can be installed to get access to the web pages. WSF continuously monitors the protected web pages and detects unauthorized manipulation to the web page. Based on customized policies, WSF can either forward the information to the protected web server, redirect the customer to an error page or disconnect the session.

WSF Attacks


Operating System
Browser Client
- HTML
- JavaScript
- DOM
- Plugins
SSL Termination
Network SSL Encrypted
DMZ / Firewall
HTTPS Gateway
WSF Server
Application Servers
SSL Encryption
WSF Protection
Sessions protected by dynamic obfuscation, additional encryption and session keys
Hidden application code and URL's
Browser and session protected by monitoring and integrity checks
Forensic Report and Attack Handling

Session Hijacking: Session inject tools, such as SQL injects in URL parameters, exploits the vulnerability in the web servers and attack by sending malicious code or data. The built-in session handling between the WSF client and the WSF server ensures that only data from the WSF client is passed to the protected web server. In addition the encryption of URL's further protects the visibility and potential vulnerabilities of the web server and set-up

CodeSealer A/S

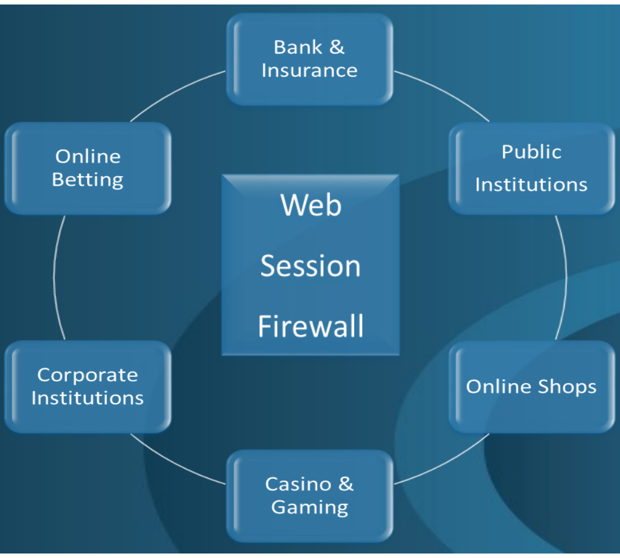
CodeSealer A/S is an international, privately held company with head office in Copenhagen, Denmark - your partner in Web Session Protection.

The company was founded by Martin Boesgaard, a well known name within the IT security industry. Today, the company is owned by a group of private investors.

The company provides two products, WSF and Bootloader. The Bootloader is presently being used within solutions countrywide, in Denmark and Norway, by more than 12 million customers daily. References can be obtained upon request.

CodeSealer A/S holds technology patents within key markets and offers a unique solution to your security needs.

The company originated within the financial sector, which has been the priority during the initial years, but today the customer base spreads to both public and corporate institutions.



CUSTOMERS

- Banking and Financial Institutions
  - Financial and Sensitive Data
- Governments and Public Institutions
  - Personal and Tax Sensitive Data
- Corporate Institutions
  - Customer and Company Data
- Casino & Gaming
  - Financial and User Data
- Online Shops
  - Login, User and Financial Data

CONTACTS

Tonny Rabjerg

CEO & CIO

Tonny has a broad international leadership experience within IT. Working for more than 30 years with application development and operation within companies such as SAS, Amadeus, Star Alliance and Danske Bank, he has a deep insight in IT Management. In his latest role, Tonny was responsible for the establishment of Danske Bank's IT and Support Services India and Danske Banks' sourcing in India, managing more than 850 people.

Phone: +45 2099 9984
eMail: tr@codesealer.com

Elisabeth Reichwald

CFO

Elisabeth has extensive experience working for companies such as Dansk Datamatik Center, C.W. Obel, and most recently, Deloitte, where she was responsible for financial reporting and administrative functions. Elisabeth holds a bachelor degree in finance from Copenhagen Business School

Phone: +45 2099 9985
eMail: er@codesealer.com

Our Team

Our Research and Development team includes specialists within the field of IT security and the financial sector. The specialists have master degrees in computer science and are specialized in design of solutions, using Go, Java and JavaScript.

Sales & Administration: +45 7199 2899
Support: +45 2594 2224
eMail: info@codesealer.com /
support@codesealer.com