

PRIMEINK TOOLBOXES



e-Security Tools for
Professional Application Development



CRYPTOMATHIC
e-Security for Better Business

E-SECURITY TOOLS FOR PROFESSIONAL APPLICATION DEVELOPMENT

Application Security

The Primelnk family of toolboxes enables you to secure any type of business application. This is a pre-requisite for doing e-Business further widening the range of business that that can be done electronically, but also it is a tool to secure data inside your organisation.

Business applications must be secure in order to protect yourself, your business partners and your customers against direct threats like fraud and espionage. But e-Security can also be used to build trust between parties allowing them to fully benefit from doing e-Business.

Depending on your actual needs, you can secure applications and transactions on all levels, ranging from basic confidentiality to advanced and legally binding digital signature systems.

Please look through this brochure in order to find the toolbox that suits your application, and feel free to contact us for product sheets with more details on each individual toolbox and assistance of a qualified system architect.

Security Needs

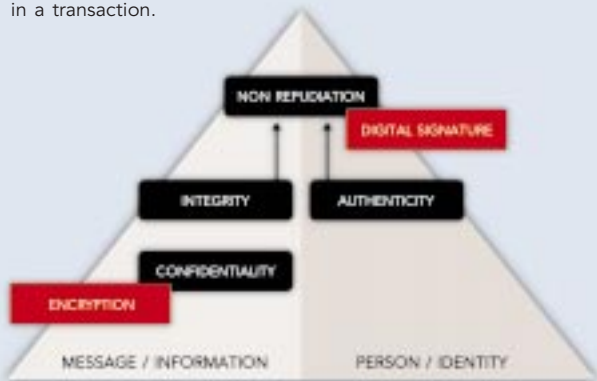
e-Security in applications can be broken down into four basic building blocks:

Confidentiality - Ensuring that only the intended party is able to read the information

Integrity - Ensuring that the information has not been modified

Authenticity - Ensuring the identity of the communicating party

Non-repudiation - Ensuring that a party cannot deny involvement in a transaction.



The illustration shows that a digital signature assures both the integrity of a message and the authenticity of a sender. This makes non-repudiation and binding transactions possible.

Security Means

Two central technical means to address these security needs are:

Encryption - To achieve confidentiality

Digital Signature - To achieve integrity, authenticity, and non-repudiation; hence making it possible to enter legally binding transactions

Primelnk e-Security Tools

Primelnk is a new range of toolboxes for securing business applications.

Primelnk provides the security you need whether you are developing for an open or controlled environment, whether the application is used internally or externally, and regardless of the platform used.

System integrators, architects, and developers can benefit from the Primelnk family. Each toolbox is targeted for a specific application type. Just pick the toolbox that meets your security requirements and fits your application architecture, and you will have everything needed for securing the application.

Primelnk is simple to purchase. A license can be obtained for a single customer solution, for an entire organisation, or for OEM software development. There are no limitations on the number of application developers or the number of end users.

Secure - Built by world-class security experts and deployed by numerous customers within all industries.

Portable - Primelnk has been deployed on various platforms ranging from mainframes to the smallest handheld and embedded devices. Platform independent code with a small footprint and our expertise in understanding security in various environments set virtually no limit.

Fast - Primelnk is optimised for performance and is among the absolutely fastest in the market. Additionally, we offer a high-speed native version written in assembler for the Intel platform.

Hardware Crypto Enabled - For physical security and even better performance, Primelnk optionally supports specialised hardware security modules, accelerators, and smart cards.

Compliant - Primelnk supports all relevant security standards.

Sensitive Memory Management - Ensures that all temporary storage of sensitive data is erased after use.

Language Availability

The Primelnk toolboxes* are available for a series of platforms including: Windows 95/98/NT/2000/CE, Linux, Mac OS, Palm OS, Sun Solaris, HP-UX, IBM AIX, OS/2, OS/400, and OS/390. Source code in ANSI C can be delivered.

Selected toolboxes are also available in a Java version.

* With the exception of Primelnk for Web Applications and Primelnk add-on: High-Speed Native Crypto

TOOLBOXES

Primelnk Conventional Cryptography

Conventional cryptography is a security cornerstone which addresses the need to protect data (in storage and on a network) against unauthorised access and modification. Applications that can be secured with conventional cryptography are e.g. protection of files on PCs, secure communication on networks within your own organisation, or applications with a need for secure pre-defined connections.

The toolbox is available for ANSI C and for Java.

This toolbox provides security for e.g.:

- Personal file encryption
- Hard disk encryption
- Communication with predefined connections
- Communication tunnels, like in Virtual Private Networks (VPN)
- Ad-hoc file exchange

Primelnk for Client/Server Applications

Distributed applications conforming to a client/server or comparable architecture can be secured with Primelnk for Client/Server Applications. The toolbox provides building blocks to ensure confidentiality and integrity; it protects data in storage and on a network against unauthorised access and modification. Also user or system authenticity can be ensured through dynamically established connections or relations. Primelnk for Client/Server Applications is best fitted for applications in a controlled environment, e.g. within your own organisation.

The toolbox is available for ANSI C and for Java.

This toolbox provides security for e.g.:

- Communication with dynamic connections
- Remote network or system access
- Access control systems
- System Management applications

Support

Our experienced security experts can provide you with professional guidance, and help you through installation and usage of Primelnk.

Maintenance
Our maintenance agreement gives you any new product version with all new algorithms and interfaces. Additionally, we notify you in the event of a security flaw as soon as it has been detected and verified, and again when a correction is available. This gives you an unprecedented level of long-term security.

Primelnk for B2B Communication

Communication between people is to a great extent satisfied through e-mails. Business-to-business communication, however, often raises the need for more structural information exchange. This need is a major motivation for using XML or EDifact for exchanging information between businesses.

Primelnk for B2B Communication is a toolbox for securing exchange of structured information.

This toolbox provides security for e.g.:

- Marketplace and procurement applications
- Inter-company information exchange
- Invoicing
- Automated reporting

Primelnk Secure Mail for Applications (S/MIME)

By using e-mail for business applications, the need to handle trusted communication by other applications than standard mail clients arises. Primelnk Secure Mail for Applications is the building block which enables application servers to secure sent and received e-mails, whether these are encrypted for confidentiality, or signed for authenticity, integrity, and non-repudiation.

This toolbox provides security for e.g.:

- Reporting applications
- Subscription applications
- Central processing of secure e-mail
- Automated e-mail notification



Primelnk for Web Applications

An e-Business application can be enabled to provide a trustworthy digital signature for documents and transactions. This widens the range of application, increases trust and enables legally binding transactions. Primelnk for Web Applications enables web based applications to work with digital signatures. Based on an electronic identity issued by a trusted 3rd party, a web user applies a personal signature to a document. The application server then validates the signature and identity, hence assuring integrity, authenticity, and non-repudiation.

This toolbox provides security for e.g.:

- Form based applications
- Web reporting
- Citizen self-service
- Marketplace and procurement applications

Primelnk Internet Protocols (SSL/TLS)

Primelnk Internet Protocols is the building block needed for building applications which exploits Internet security standards. It provides confidentiality, integrity, and authentication at network communication level.

Applications can be enabled to communicate with existing web browsers and servers, or the protocols can be used for distributed applications, e.g. conforming to client/server architecture.

This toolbox provides security for e.g.:

- Transport level security for applications
- Client- or serverside SSL/TLS enabling
- Automated subscription to:
 - anti virus updates
 - product catalogue data
 - software updates

Primelnk for Mobile Applications

Primelnk for Mobile Applications provides security based on the innovative Elliptic Curve Cryptography. This is particularly suitable for securing applications and communication in constrained and in highly optimised environments:

Constrained environments are devices characterised by less computing power, less memory, and slower communication capabilities than ordinary PCs.

Optimised environments require particularly high performance in cryptographic computations.

This toolbox provides security for e.g.:

- Constrained environments
- Highly optimised solutions
- Communication with:
 - next generation phones
 - PDA devices
- Handheld device applications and protocols

Education

Cryptomathic's modular education programme is based on 15 years of experience. We offer education in e-Security ranging from general introductions to expert level workshops.

Primelnk Premium for PKI

A Public Key Infrastructure (PKI) is the most advanced and flexible security solution and is particularly suitable for applications deployed in open environments. PKI defines an infrastructure with trusted 3rd parties: A Certificate Authority (CA) and an optional Time Stamping Authority (TSA). Primelnk Premium for PKI provides what's needed to enable applications for PKI. This includes electronic identities (certificates) for authenticity, digital signatures and optional time stamping for non-repudiation, and recipient-specific encryption for confidentiality.

This toolbox provides security for e.g.:

- Applications deployed outside a controlled environment
- Interoperable security solutions
- Access control in open environments
- Home banking
- Internet based groupware

Primelnk add-on: High-Speed Native Crypto

Performance can be a critical parameter for ensuring system scalability and fast response times. Security components can be tuned by using Primelnk High-Speed Native Crypto which is an extremely optimised implementation.

Primelnk High-Speed Native Crypto introduces a native assembler code implementation of the most common cryptographic algorithms. It provides a performance improvement of between 50 and 300 per cent.

The toolbox add-on is designed for the Windows/Intel platform.

This toolbox is applicable to:

- Primelnk Conventional Cryptography
- Primelnk for Client/Server Applications
- Primelnk Secure Mail for Applications (S/MIME)
- Primelnk Premium for PKI
- Primelnk Internet Protocols (SSL/TLS)
- Primelnk for Mobile Applications
- Primelnk for B2B Communication

Consultancy
Our experienced consultants offer strategic level advice, analysis and design of e-Security architecture, as well as product installation and integration into your own applications.



Primelnk add-on: Crypto Hardware Support

Some scenarios require an extraordinary high level of physical security and/or the highest available performance. This toolbox add-on enables support for two different types of crypto hardware: Hardware Security Modules/Accelerators and smart cards.

A Hardware Security Module provides physical security; a dedicated Hardware Crypto Accelerator gives the performance a boost, while some modules provide both enhancements.

Smart cards give users a place to store secret and private encryption keys. They offer better security than typical solutions which use the system hard disk for storage.

This toolbox is applicable to:

- Primelnk Secure Mail for Applications (S/MIME)
- Primelnk Premium for PKI
- Primelnk Internet Protocols (SSL/TLS)
- Primelnk for B2B Communication

About Cryptomathic

With more than 15 years of experience, Cryptomathic is one of the world's leading providers of e-Security. We can assist you in securing your business by providing best-of-breed e-Security software products, consultancy, education, and complete security solutions.

Our range of software products covers toolboxes for professional application development, PKI trust products as well as pre-personalisation of payment smart cards.

Cryptomathic's world-class experts offer e-Security consultancy at strategic level, for solution architecture, and integration.

We offer a complete modular education program, where you can learn what you need to know about e-Security – both on a general and product specific level.

All our products are continuously updated and extended, based on the most recent developments in the business. A maintenance agreement guarantees such periodic updates.

Product support agreements offer supplementary expert guidance for installation and usage of our software products.

We serve our customers through our head office in Denmark and our European subsidiaries.

For more information, please mail us at primeink@cryptomathic.com or visit our web site:

www.cryptomathic.com

Cryptomathic A/S
Kannikegade 14, 3
DK-8000 Aarhus C
Denmark
Tel. +45 8613 9020
Fax +45 8620 2975

Cryptomathic A/S
Christians Brygge 28, 2
DK-1559 Copenhagen V
Denmark
Tel. +45 8613 9020
Fax +45 8620 2975

Cryptomathic NV
Lei 8A
B-3000 Leuven
Belgium
Tel. +32 (0) 16 300 880
Fax +32 (0) 16 389 452

Cryptomathic Italia S.p.A.
Corso Svizzera, 185
I-10149 Torino
Italia
Tel. +39 0 11 7509527
Fax +39 0 11 7509535

Cryptomathic Ltd
St. John's Innovation Centre
Cowley Road
Cambridge CB4 0WS
United Kingdom
Tel. +44 (0) 1223 421399
Fax +44 (0) 1223 421984