

CRYPTOMATHIC

**Cryptomathic PrimeInk
Technical Brochure**

Trademarks

All brand names and product names are trademarks or registered trademarks of their respective owners.

Copyrights

Under copyright law, this document may not be copied, photocopied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of Cryptomathic A/S.

Disclaimer

Cryptomathic may make improvements and/or changes to the product described in this brochure at any time. The brochure is not part of the documentation for a specific version or release of the product, but will be updated periodically.

Contact

If you wish to obtain further information on this product or any other Cryptomathic product, please visit our web site or contact your regional Cryptomathic branch.

www.cryptomathic.com

Cryptomathic A/S
Jægergårdsgade 118
DK-8000 Aarhus C
Denmark
Tel. +45 8676 2288
Fax +45 8620 2975

Date: 2007-03-14
Doc. title: PrimeInk Technical Brochure
Doc. version: 1.0.3



Table of Contents

Table of Contents.....	3
1 Overview.....	5
1.1 Introduction.....	5
1.2 Key Features	6
1.3 The PrimeInk Family	7
1.4 Language and Interface	8
ANSI C Toolkits.....	8
Java Toolkit.....	8
Other Toolkits.....	9
2 Universal Toolkits.....	10
2.1 PrimeInk Basic	10
2.2 PrimeInk Premium.....	11
2.3 PrimeInk Java.....	12
2.4 PrimeInk ECC.....	13
3 Application-Specific Toolkits.....	14
3.1 PrimeInk Web Signer	14
3.2 PrimeInk Signature Validator	15
3.3 PrimeInk Secure Mail	16
3.4 PrimeInk CSP.....	17
4 PrimeInk Add-Ons	18
4.1 Hardware Crypto Support	18
4.2 High-Speed Assembler Support.....	19
Appendix A: Technical Specification Summary.....	20
Appendix B: PrimeInk Performance.....	22
Hash Algorithms (kbit/sec).....	22
Algorithm.....	22
Pure ANSI C	22
Mixed	22
Pure Assembler.....	22
Symmetric Algorithms (kbit/sec)	22
Algorithm.....	22
Pure ANSI C	22
Mixed	22
Pure Assembler.....	22
RSA Public-Key Operations (operations/sec)	23
Parameters	23
Pure ANSI C	23
Mixed	23
Pure Assembler.....	23
RSA Private-Key Operations (operations/sec).....	23
Parameters	23



Pure ANSI C	23
Mixed	23
Pure Assembler.....	23
RSA Key Pair Generation (sec).....	23
Parameters	23
Pure ANSI C	23
Mixed	23
Pure Assembler.....	23
ECC Signature Generation Char. 2 (operations/sec)	24
Parameters	24
Pure ANSI C	24
Mixed	24
Pure Assembler.....	24
ECC Signature Verification Char. 2 (operations/sec)	24
Parameters	24
Pure ANSI C	24
Mixed	24
Pure Assembler.....	24
ECC Signature Generation Char. P (operations/sec).....	24
Parameters	24
Pure ANSI C	24
Mixed	24
Pure Assembler.....	24
ECC Signature Verification Char. P (operations/sec).....	24
Parameters	24
Pure ANSI C	24
Mixed	24
Pure Assembler.....	24



1 Overview

1.1 Introduction

Business applications must be secure in order to protect yourself, your partners and your customers against direct threats such as fraud and espionage. In addition, by creating a trusted electronic business environment, organisations can open new market channels and realise significant cost savings.

Cryptomathic PrimeInk is a range of toolkits for securing a wide variety of business applications. A result of almost 20 years of experience in delivering security solutions, PrimeInk offers high performance combined with ease of integration through compliance with all relevant security standards.

For applications ranging from secure data storage and communication, to trusted web-based forms, there is a PrimeInk toolkit that can provide a simple solution. PrimeInk has been deployed worldwide in applications as diverse as data encryption utilities to advanced and legally-binding digital signature solutions.

System integrators, architects and developers can all benefit from using PrimeInk. Each toolkit is targeted for a specific application type – just pick the toolkit that meets your security requirements and fits your system architecture, and you will have everything needed to secure your application.

Please look through this brochure to see the technical details of the toolkits that we offer. There is also an overview brochure for the less technical audience. Feel free to contact us with any questions on the individual toolkits or for the assistance of a qualified security architect. Contact information can be found on page 2.



1.2 Key Features

PrimeInk offers the following key features:

- **Secure**
PrimeInk is built by world-class security experts and incorporates industry standard algorithms and best-of-breed security features.
- **Proven**
PrimeInk has been deployed worldwide within all industry sectors.
- **Portable**
PrimeInk can easily be deployed on a wide range of platforms including mainframes, PCs, handhelds, embedded devices and smart cards. The efficient program code is written in standard ANSI C or Java for optimal platform independence.
- **Compliant**
PrimeInk supports all current relevant security standards, and continues to evolve as new standards are developed and adopted.
- **Fast**
PrimeInk is highly optimised for performance making it one of the fastest cryptographic implementations on the market. Additionally, we offer a high-speed assembler add-on package for even higher performance with selected algorithms.
- **Flexible**
PrimeInk toolkits are applicable across all scenarios where cryptographic security techniques are required, and offer tailored solutions to common business security problems.
- **Hardware Enabled**
For physical security and even better performance, PrimeInk optionally supports specialised hardware security modules, accelerators, and smart cards. A common interface makes migration from software to hardware or between hardware devices straightforward.
- **Source Code**
PrimeInk is delivered with complete source code, making integration into your existing development environment as simple and straightforward as possible. Furthermore, this openness makes it easy to inspect our code for possible backdoors or weaknesses.

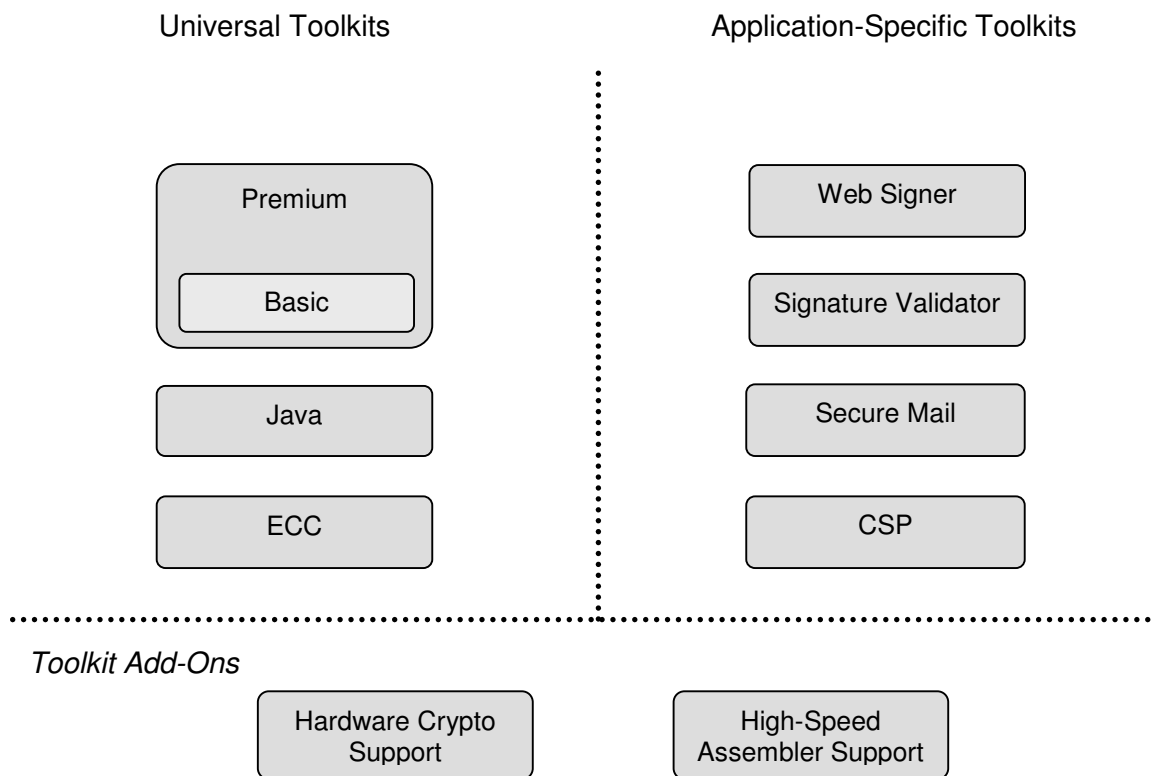


1.3 The PrimeInk Family

The PrimeInk toolkits are divided into three groups:

- Universal Toolkits – Standards-based cryptographic algorithm implementations that are widely applicable across a range of applications.
- Application-Specific Toolkits – Tailored toolkits providing a plug-in solution to a specific common security requirement.
- Toolkit Add-Ons – Enhancements to the above toolkits adding support for additional features to address particular specialised requirements.

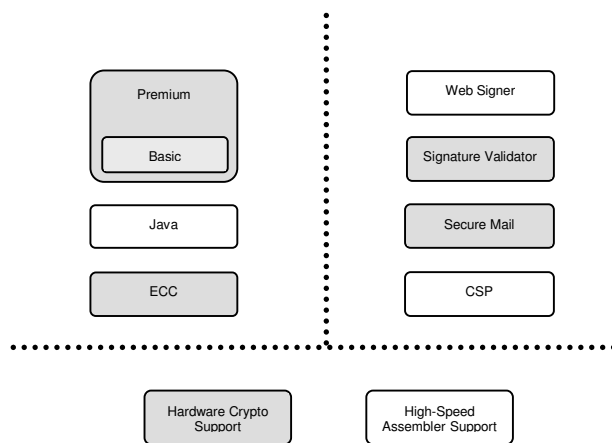
The toolkits within each group are shown in the diagram below:



1.4 Language and Interface

PrimeInk is designed to be easy to use and to be readily portable to a variety of platforms. This philosophy is seen in the choice of programming interface offered and language used for the code, as described in the following section. For your convenience, the toolkits are delivered with source code to let you compile and link as desired in any development environment. Furthermore, this gives you the opportunity to inspect the code for backdoors and other weaknesses.

ANSI C Toolkits



The majority of the PrimeInk toolkits and add-ons are written in pure ANSI C and include features to allow platform portability such as big-endian/little-endian and support for the EBCDIC character set. As such, these toolkits are available for a wide range of platforms including: Windows 95/98/Me/NT/2000/XP/CE, Linux, Mac OS, Sun Solaris, HP-UX, IBM AIX, OS/2. The code has also been successfully compiled and run on IBM iSeries and zSeries machines.

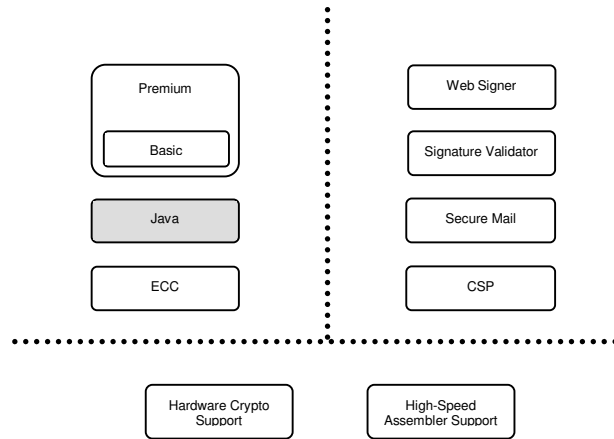
Since release 6.0, the Basic, Premium and Secure Mail toolkits have provided a new and powerful programming interface: the Crypto Programming Interface (CPI). This interface provides the programmer with an easily understandable entry point to cryptographic operations. CPI separates the application calling the cryptographic routines from their internal implementation. Different implementations in the form of CPI 'providers' may therefore be used with minimal changes to the application code.

Java Toolkit

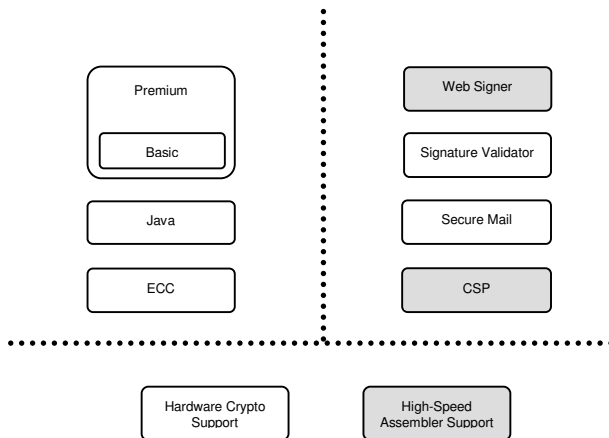
PrimeInk Java is written in 100% pure Java and compatible with any Java Virtual Machine (JVM) - version 1.4 or later. Thanks to the platform independence of Java, this toolkit can be run on almost any platform. It is delivered as a signed provider which is accessed via the standard Java Cryptography Extension (JCE) interface. The Java source code is also delivered.



In addition, the ANSI C toolkits can easily be used from Java through the Java Native Interface (JNI). Specifically, PrimeInk Signature Validator is delivered with such a JNI wrapping.



Other Toolkits



The remaining toolkits and add-ons are designed for specific platforms.

PrimeInk Web Signer consists of two signing components:

- An ActiveX object for Microsoft Internet Explorer.
- A Java applet for other browsers (with the Sun JRE, version 1.4 or later).

Both components are interfaced from a web page using VBScript, JavaScript or similar.

PrimeInk CSP is a Microsoft Windows component, interfaced through the Microsoft Crypto API (MS CAPI) provided as a part of the operating system.

PrimeInk High-Speed Assembler Support is written in pure, hand-optimised assembler for the Windows/x86 platform. The assembler code replaces a few .c files and the interface remains unchanged.

2 Universal Toolkits

2.1 PrimeInk Basic

PrimeInk Basic features a full range of cryptographic algorithms that are widely used today. These are broadly applicable across a wide range of application scenarios, including ensuring the confidentiality and protecting the integrity of any application data. In networked environments, PrimeInk Basic can be used for authenticating users and for protecting the confidentiality and integrity of data in transit.

The toolkit is written in pure ANSI C for maximum portability. It is optimised for high performance and features inline assembler implementations of critical mathematical routines for additional speed on x86 processors.

The Cryptomathic CPI provides easy access to symmetric and asymmetric encryption, hash algorithms, message authentication codes, digital signatures and common key management tasks such as generation, derivation and exchange.

Key Features	
Symmetric Algorithms	AES, DES, 3DES
Asymmetric Algorithms	RSA, DSA, ISO 9796-1
Key Management	RSA, Diffie-Hellman
Hash Algorithms	SHA-1, MD2, MD5, SHA-256/384/512, RIPEMD-160
MAC Algorithms	HMAC, CBC-MAC
Other Standards	PKCS#5
Language / Interface	ANSI C / CPI
Toolkit Add-Ons	Hardware Crypto Support, High-Speed Assembler Support



2.2 PrimeInk Premium

PrimeInk Premium offers all the features of PrimeInk Basic, plus full support for digital certificates and message formats. This allows standards-based integration with a wide range of third-party security products, as well as enabling signatures, authentication and encryption with third parties across open networks.

The toolkit is written in pure ANSI C for maximum portability. It is optimised for high performance and features inline assembler implementations of critical mathematical routines for additional speed on x86 processors.

The Cryptomathic CPI provides easy access to symmetric and asymmetric encryption, hash algorithms, message authentication codes, digital signatures and common key management tasks such as generation, derivation and exchange. Full certificate handling is supported, including path discovery and validation.

PrimeInk Premium also incorporates all of the commonly used PKCS data formats, as well as several PKIX standards and the secure e-mail standard: S/MIME. It is an ideal toolkit for the development of applications that integrate with Public Key Infrastructures (PKIs), including certificate authorities and time-stamping authorities.

Key Features	
Symmetric Algorithms	AES, DES, 3DES
Asymmetric Algorithms	RSA, DSA
Key Management	RSA, Diffie-Hellman
Hash Algorithms	SHA-1, MD2, MD5, SHA-256/384/512, RIPEMD-160
MAC Algorithms	HMAC, CBC-MAC
Certificates	X.509 v3, CRL v2, PKCS#12 (PFX)
Certificate Management	PKIX-OCSP, PKIX-CRMF, PKIX-CMP, PKIX-CMC, PKCS#10
Message Formats	CMS, PKCS#7, S/MIME
Time-Stamping	PKIX-TST
Other Standards	PKCS#1, PKCS#5, PKCS#8, PKCS#9, ISO 9796-1
Language / Interface	ANSI C / CPI
Toolkit Add-Ons	Hardware Crypto Support, High-Speed Assembler Support



2.3 PrimeInk Java

Using cryptography and security in Java applications is straight-forward using the common interface defined by Sun. PrimeInk Java is a signed Java Cryptography Extension (JCE) provider, which integrates seamlessly with the standard Java development environment. It provides a full set of highly optimised cryptographic algorithms.

The toolkit is written in 100% pure Java and runs on any Java 1.4 or later Java Virtual Machine (JVM). It offers symmetric and asymmetric encryption, hash algorithms and message authentication codes.

Key Features	
Symmetric Algorithms	AES, DES, 3DES
Asymmetric Algorithms	RSA
Key Management	RSA
Hash Algorithms	SHA-1, MD5, RIPEMD-160
MAC Algorithms	HMAC, CBC-MAC
Other Standards	ISO 9796-1
Language / Interface	Java (1.4 or later) / JCE



2.4 PrimeInk ECC

PrimeInk ECC provides security based on Elliptic Curve Cryptography (ECC). These advanced public key cryptographic algorithms achieve similar security to traditional algorithms but using much shorter keys. This makes computations faster and reduces storage requirements. In particular, key generation is considerably faster than traditional public key algorithms.

Working with elliptic curves requires the generation of curve parameters, which involves a complex procedure known as ‘point counting’. PrimeInk ECC includes highly efficient point counting routines allowing the full range of ECC operations to be supported. PrimeInk ECC is fully compliant with all relevant ECC standards. In keeping with most ECC implementations, PrimeInk ECC only supports fields of characteristic 2.

Included in the package are implementations of the AES symmetric cipher and a variety of hash algorithms, providing everything necessary for most security applications. It is supplied in ANSI C, which can be compiled to almost any platform.

Key Features	
Symmetric Algorithms	AES
Asymmetric Algorithms	ECDSA (X9.62)
Key Management	ECDH (ISO/IEEE 1363)
Key Formats	X9.62
Hash Algorithms	SHA-1, RIPEMD-160
Language / Interface	ANSI C



3 Application-Specific Toolkits

3.1 PrimeInk Web Signer

PrimeInk Web Signer makes it easy to design web applications which allow the user to create digital signatures from their browser. This enables high-value web applications for which non-repudiation of user actions is a requirement. Furthermore, the use of digital signatures may simplify application design and make it easier to satisfy specific audit requirements.

The signing components are downloaded from the web server, allowing user mobility as well as dramatically reducing deployment and maintenance costs. No code needs to be installed on the client machine. The components can be interfaced in various ways, typically with VBScript or JavaScript from within HTML. The two signing components cover almost any browser on the market. Sample code is provided with the toolkit for both components.

For Microsoft Internet Explorer, the PrimeInk Web Signer ActiveX object is used. It creates digital signatures using the Microsoft Crypto-API to access the signing key from the Windows key store, from tokens such as smart cards, or from any other installed Crypto Service Provider.

For other browsers, the PrimeInk Web Signer Java applet can be used. It accesses the signing key from a PKCS#12 (PFX) file stored locally on the user's machine.

Key Features	
Signature Format	PKCS#7
Programming Interface	JavaScript, VB Script, ...



3.2 PrimeInk Signature Validator

PrimeInk Signature Validator simplifies the task of validating digital signatures and corresponding certificates. It forms a natural companion to PrimeInk Web Signer, but can also be used to validate signatures from other sources, such as the Cryptomathic Signer or third-party signature applications.

The toolkit provides the application developer with a simple, high-level interface to achieve reliable signature validation, making it suitable for developers with little security expertise. It transparently takes care of discovering the path to a trusted root certificate and validating the entire path. This includes check for certificate revocation status and validity of certificate extensions. It allows for validation of a digital signature created with any PKCS#7 compliant device.

PrimeInk Signature Validator is supplied in ANSI C which can be compiled to almost any platform. However, it can also be used in Java applications via the Java Native Interface (JNI). Sample code is provided for both application languages.

Key Features	
Certificates	X.509 v3, CRL v2
Signature Format	PKCS#7
Programming Interface	ANSI C, JNI
Toolkit Add-Ons	Crypto Hardware Support, High-Speed Assembler Support



3.3 PrimeInk Secure Mail

PrimeInk Secure Mail enables application servers to send and receive secure e-mail, using the S/MIME standard and X.509 certificates. Secure mail offers a very simple form of integration for passing secure messages between systems, and offers e-mail recipients a high level of confidence.

The toolkit includes functions for encrypting, decrypting and digitally signing any e-mail message, as well as validating e-mail signatures. It provides a simple high level interface to the cryptographic functions required, allowing it to be used by developers with little security expertise. PrimeInk Secure Mail is supplied in ANSI C which can be compiled to almost any platform.

Key Features	
Certificates	X.509 v3, CRL v2, PKCS#12 (PFX)
Certificate Management	PKIX-OCSP
Time-Stamping	PKIX-TST
Message Formats	S/MIME
Language / Interface	ANSI C / CPI
Toolkit Add-Ons	Hardware Crypto Support, High-Speed Assembler Support



3.4 PrimeInk CSP

A Cryptographic Service Provider (CSP) is a Microsoft Windows component that offers cryptographic services such as encryption or signing and the secure storage of user keys. All CSPs are accessible via standard Microsoft interfaces, and thus integrate fully with standard Microsoft applications such as Outlook, Outlook Express and Internet Explorer, as well as third-party software such as VPN clients.

The PrimeInk CSP provides an alternative to the standard Microsoft CSPs on Windows/x86 platforms. It offers full-strength cryptographic algorithms and key protection. In addition, the PrimeInk CSP offers the application developer full control of the user experience regarding password policies and the dialog branding.

The CSP uses strong encryption (128 bit AES) for effective protection of the key store against brute force attacks, and is also capable of enforcing the use of a password of a given strength. It has been digitally signed by Microsoft, making for straightforward deployment on any Windows PC.

To make key management simpler, we provide an ActiveX utility which is capable of changing passwords, importing and exporting keys in PKCS#12 (PFX) format, and handling certification requests/responses in PKCS#10 and PKCS#7 format.

Key Features	
Symmetric Algorithms	AES, DES, 3DES
Asymmetric Algorithms	RSA
Key Management	RSA
Hash Algorithms	SHA-1, MD2, MD5
Programming Interface	Microsoft Crypto API (MS CAPI)



4 PrimeInk Add-Ons

4.1 Hardware Crypto Support

Some scenarios require an extraordinary high level of physical security and/or the highest available performance. This add-on enables support for all PKCS#11 based hardware. Compatible hardware includes hardware security modules from leading manufacturers and also smart card readers and USB key tokens from all main vendors.

Also included is a PKCS#11 interface to PrimeInk, which allows it to act as a software PKCS#11 device. This can be used in applications which have a PKCS#11 interface for cryptographic action but where no hardware PKCS#11 token is available, or during development to avoid the cost of deploying expensive cryptographic hardware on every workstation. Whether using hardware or software implementations, the PrimeInk programming interface remains the same.

PrimeInk Hardware Crypto Support plugs into the Crypto Programming Interface (CPI) used by the ANSI C PrimeInk toolkits. With this add-on, the CPI architecture interfaces to the PKCS#11 provider supplied with the device. This common interface allows application developers to migrate easily from software-based to hardware-based cryptographic calls, without having to make any significant code changes.

Being able to use PrimeInk as a software PKCS#11 device allows it to function as a plugin replacement for an existing provider. Additionally, developers benefit from the ability to debug function calls 'into' the device during application testing.

Key Features	
Symmetric Algorithms	DES, 3DES
Asymmetric Algorithms	RSA, DSA
Key Management	RSA, Diffie-Hellman
Hash Algorithms	SHA-1, MD5
Language / Interface	ANSI C / CPI, PKCS#11



4.2 High-Speed Assembler Support

Performance can be a critical parameter for ensuring system scalability and fast response times. For the fastest possible performance on Windows/x86 platforms, this add-on provides highly-optimised assembler implementations of the most common cryptographic algorithms. The performance boost is typically between 50 and 100 percent. This add-on is a plug-in enhancement to the existing PrimeInk toolkits, with no interface changes and thus no additional development is required.

For further details on performance, please refer to Appendix B.

Key Features	
Symmetric algorithms	DES, 3DES
Asymmetric Algorithms	RSA, DSA
Key Management	RSA, Diffie-Hellman
Hash Algorithms	SHA-1, MD2, MD5, RIPEMD-160
Language / Interface	x86 assembler / CPI



Appendix A: Technical Specification Summary

Key:

- ✓ Provided as a main component.
- o Provided as a sub-component, but with a license to use only within the package constraints.
- ^C Use of the algorithm is recommended only for backwards compatibility.
- ^L Use of the algorithm is available through low-level functions.
- ¹ Only for algorithms included in the package.

		Universal Toolkits				Application -Specific Toolkits				Toolkit Add-Ons	
		Basic	Premium	Java	ECC	Web Signer	Signature Validator	Secure Mail	CSP	Hardware Crypto Support	High-Speed Assembler Support
Symmetric Algorithms											
AES	FIPS 197	✓	✓	✓	✓			o	✓		
DES ^C	X3.92	✓	✓	✓				o	✓	✓	✓
3DES	X9.52	✓	✓	✓				o	✓	✓	✓
Asymmetric Algorithms											
RSA	FIPS 186-2	✓	✓	✓		o	o	o	✓	✓	✓
DSA	FIPS 186-2	✓	✓					o		✓	✓
ECDSA	X9.62				✓						
Key Management											
RSA	PKCS#1 v1.5	✓	✓	✓				o	✓	✓	✓
Diffie-Hellman	X9.42	✓	✓					o		✓	✓
ECDH	IEEE P1363				✓						
Hash Algorithms											
SHA-1	FIPS 180-2	✓	✓	✓	✓	o	o	o	✓	✓	✓
MD2	RFC 1319	✓	✓					o	✓		✓
MD5 ^C	RFC 1321	✓	✓	✓				o	✓	✓	✓
SHA-256/384/512	FIPS 180-2	✓	✓					o			
RIPMD-160	ISO/IEC 10118-3	✓	✓	✓	✓			o			✓
MDC2 ^L , MDC4 ^L	ISO/IEC 10118-2	✓	✓	✓				o			✓
MAC Algorithms											
HMAC	FIPS 198	✓	✓	✓				o			
CBC-MAC	FIPS 113	✓	✓	✓				o			
MAC ^L	ISO 9797	✓	✓					o			
Certificates											
X.509 v3	RFC 3280		✓				✓	✓			
CRL v2	RFC 3280		✓				✓	✓			
PKCS#12 v1.0 (PFX)			✓					✓			



		Universal Toolkits			Application -Specific Toolkits			Toolkit Add-Ons		
Certificate Management										
PKIX-OCSP	RFC 2560	✓				✓				
PKIX-CRMF	RFC 2511	✓								
PKIX-CMP	RFC 2510	✓								
PKIX-CMC	RFC 2797	✓								
PKCS#10 v1.0		✓								
Message Formats										
S/MIME v3	RFC 2632, 2633	✓				✓				
CMS	RFC 3217, 3369, 3370, 3394, 3560, 3565	✓								
PKCS#7 v1.5		✓			✓	✓				
Time-Stamping										
PKIX-TST	RFC 3161	✓				✓				
Digital Signature Applications										
Web Signatures (ActiveX object and Java applet)						✓				
Validation API							✓			
Other Standards										
PKCS #1 v2.1		✓					o			
PKCS #5 v2.0		✓	✓				o			
PKCS #8 v1.2		✓					o			
PKCS #9 v1.1 + additional relevant attributes		✓					o			
ISO 9796-1		✓	✓	✓			o			
Language / Interface										
ANSI C		✓	✓		✓	o	✓	✓		✓
CPI ¹		✓	✓					✓		✓
Java v1.4 (JCE)				✓			JNI			
PKCS #11 ¹										✓
Microsoft Crypto API (MS CAPI)									✓	
Utilities										
ASN.1 BER/DER	X.680 and X.690	✓					o			
Fast Large Integer Arithmetic		✓	✓				o			
Toolkit Add-On Compatibility										
Hardware Crypto Support		✓	✓				✓	✓		
High-Speed Assembler Support		✓	✓				✓	✓		



Appendix B: PrimeInk Performance

Disclaimer

The figures are intended only as an indicative guide to PrimeInk performance in general. The performance achieved in practice will vary between systems. For precise figures, we recommend testing PrimeInk on the target system itself.

Test Environment

Testing was performed on a PC with an Intel 2.4 GHz Pentium 4 processor, running Microsoft Windows 2000 SP4. All tests are pure memory-to-memory operations, with sufficient memory available so that disk and other peripherals do not influence the results.

Implementations

There are up to three implementations for each algorithm:

- 1) **Pure ANSI C** For the ultimate in portability to almost any platform.
- 2) **Mixed** ANSI C with inline assembler optimisations for key routines (enabled using the 'DDIG' compiler option). Available for any x86 platform.
- 3) **Pure Assembler** For the maximum performance on Windows/x86 platforms.

For applications where performance is critical, Cryptomathic can also provide optimised solutions tailored to a particular target platform.

Performance Tables

Hash Algorithms (kbit/sec)			
Algorithm	Pure ANSI C	Mixed	Pure Assembler
SHA-1	439560	-	568720
MD5*	1995013	-	2103418
MDC2	25221	-	42083
RIPEMD-160	438757	-	697674

Symmetric Algorithms (kbit/sec)			
Algorithm	Pure ANSI C	Mixed	Pure Assembler
AES	315271	-	-
DES*	178273	-	240602
3DES	57658	-	80301

* The MD5 and DES algorithms are recommended for backwards compatibility only.



RSA Public-Key Operations (operations/sec)				
Parameters		Pure ANSI C	Mixed	Pure Assembler
random e	1024-bit	31.8	61.5	59.3
	2048-bit	4.5	15.6	8.5
	3072-bit	1.4	4.1	2.4
	4096-bit	0.6	1.7	1.1
$e = 3$	1024-bit	13333	12315	23697
	2048-bit	4000	4444	7813
	3072-bit	1832	2463	4000
	4096-bit	1066	1048	2370
$e = 65537\dagger$	1024-bit	1938	2137	3559
	2048-bit	525	1600	1103
	3072-bit	259	395	467
	4096-bit	151	311	296

RSA Private-Key Operations (operations/sec)			
Parameters	Pure ANSI C	Mixed	Pure Assembler
1024-bit	58	213	213
2048-bit	17	27	27
3072-bit	5	6	11
4096-bit	2	6	4

RSA Key Pair Generation (sec)			
Parameters	Pure ANSI C	Mixed	Pure Assembler
1024-bit	0.030	0.025	0.016
2048-bit	0.155	0.085	0.085
3072-bit	0.621	0.229	0.254
4096-bit	2.242	0.427	0.991

† The most commonly-used value of e .



ECC Signature Generation Char. 2 (operations/sec)			
Parameters	Pure ANSI C	Mixed	Pure Assembler
163-bit	321	291	291
233-bit	116	183	182
283-bit	116	75	116
409-bit	51	58	61
571-bit	21	15	23

ECC Signature Verification Char. 2 (operations/sec)			
Parameters	Pure ANSI C	Mixed	Pure Assembler
163-bit	145	151	145
233-bit	85	91	75
283-bit	58	60	60
409-bit	29	29	32
571-bit	11	11	12

ECC Signature Generation Char. P (operations/sec)			
Parameters	Pure ANSI C	Mixed	Pure Assembler
192-bit	400	290	531
224-bit	320	177	454
256-bit	265	177	403
384-bit	114	100	177

ECC Signature Verification Char. P (operations/sec)			
Parameters	Pure ANSI C	Mixed	Pure Assembler
192-bit	106	59	138
224-bit	69	53	110
256-bit	59	42	88
384-bit	25	21	41

