CRYPTOMATHIC
www.cryptomatic.com

Cryptomathic PrimeInk Toolkits

HIGH PERFORMANCE CRYPTO TOOLS

Security is important to all businesses, to ensure the confidentiality, integrity and authenticity of both internal and customer-facing interactions. In addition, by creating a trusted business environment organisations can open up new market channels and realise significant cost savings.

Cryptomathic PrimeInk is a range of toolkits for system integrators, architects and developers to secure a wide variety of business applications. PrimeInk provides high performance, ease of integration and portable code, compliant with industry standard algorithms and proven in developments worldwide. The toolkits cover low-level cryptographic functions as well as more specific technologies such as digital signatures.

PRIMEINK TOOLKITS

PrimeInk Premium

PrimeInk Premium features a full range of cryptographic algorithms 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.

PrimeInk Premium is an ideal toolkit for the development of applications that integrate with a Public Key Infrastructure (PKI). Full X.509 certificate handling is supported, including path discovery and validation. Standard data formats for interoperation with certificate authorities and time-stamping authorities are also included.

Example applications include:

- Access control in open environments
- Interoperable security solutions
- Internet based groupware

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.

These features make PrimeInk ECC ideal for developers working with applications in low memory or performance critical environments.

Example applications include:

- Performance critical systems
- Interoperability with other ECC systems

PrimeInk Java

Using cryptography and security in Java applications is straight-forward using the common interface defined in the language. 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.

Example applications include:

- Securing J2EE and EJB enterprise applications
- Browser-based Java applets
- Secure communication for Java applications

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 and Internet Explorer, as well as third-party software such as VPN clients.

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

Example applications include:

- Customised secure email interface
- Customised secure web signing interface
- Customised VPN logon

KEY FEATURES

Secure

Primelnk Toolkits incorporate industry standard algorithms and world blass security featues.

Proven

Primelnk Toolkits have been deployed worldwide within all industry sectors.

Portable

Primelnk Toolkits 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

Primelnk Toolkits support all current relevant security standards, and continues to evolve as new standards are developed and adopted.

Fast

Primelnk Toolkits are highly optimised for performance making them one of the fastest cryptographic implementations on the market. Additionally, we offer the High-Speed Assembler add-on package for even higher performance with selected algorithms.

Flexible

Primelnk 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, Primelnk Toolkits optionally support specialised hardware security modules, accelerators, and smart cards. A common interface makes migration from software to hardware or between hardware devices straightforward.

Ease of Integration

Primelnk Toolkits are 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.

TOOLKIT ADD-ONS

Primelnk Crypto Hardware 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 cards and USB tokens from all main vendors.

Also included is a PKCS#11 interface to Primelnk, 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 Primelnk programming interface remains the same.

A technical brochure is also available for the toolkits – please contact Cryptomathic for further information.

```
int f2pol_reduceBW( dig * a, f2poly * b, const f2field * field )
{
  int i, j, k, m;
  dig *u;
  dig *r;
  unsigned long usize, l;

  if ( a[0] == 0 ) {
    memset( b, 0, ( field->digs_in_f + 1 ) * sizeof( dig ) );
    return CODE_OK;
  }

  r = map_xalloc( DIGS( field->f[0] ) );
  if ( r == NULL ) {
    return CODE_NO_MEM;
  }
  map_copy( field->f, r );
  map_clearbit( r, field->Df );
  usize = r[0] + 1;

  u = map_xalloc( usize * WS );
  if ( u == NULL ) {
    return CODE_NO_MEM;
  }
  memset( u, 0, usize * WS * sizeof( dig ) );
  for ( i = 0; i < WS; i++ ) {
    memcpy( u + ( usize * i ), r + 1, r[0] * sizeof( dig ) );
    map_sleft( r, 1 );
  }

  m = field->Df;
  for ( i = map_topb( a ); i >= m; i-- ) {
    if ( map_testbit( a, i ) == 1 ) {
      j = ( i - m ) / WS + 1;
      k = ( i - m ) % WS;
      for ( l = 0; l < usize; l++ ) {
        a[j + l] = a[j + l] ^ u[usize * k + l];
      }
      map_clearbit( a, i );
    }
  }
```

ABOUT CRYPTOMATHIC

Cryptomathic is one of the world's leading providers of security solutions to businesses across a wide range of industry sectors, including finance, smart card, digital rights management and government. With over 20 years' experience, Cryptomahtic provides customers with systems for e-banking, PKI initiatives, card personalization, ePassport, card issuing and advanced key management utilizing best-of-breed security software and services. Cryptomathic prodes itself on its strong technical expertise and unique market knowledge. Together with an established network of partners, Cryptomathic assists companies around the world with building security from requirement specification to implementation and delivery.

Learn more at cryptomathic.com