Multipass
Mobile Device Security

The Multipass security client from Blueice Research allows for the provision of value added services on the mobile Internet. It is a cross-platform security client that brings strong encryption functionality to a variety of mobile device and PC platforms. It allows users, corporations and service providers the ability to perform secure transactions while conducting business on-line. The Multipass application is based on open Public Key Infrastructure standards.

About Blueice Research

Blueice Research, founded in February 2000, is a software security company. From its headquarters in Stockholm, Sweden, Blueice Research develops and markets infrastructure security products that enable secure electronic transaction on mobile devices.

The development of mobile devices such as smart phones and Personal Digital Assistants has opened the way for new Internet-based services requiring strong security. Blueice Research is at the forefront in the development of these solutions bringing advanced security functionality to the world of wireless devices.

Blueice Research is an active contributor to the leading forums for the advancement of mobile security including the Mobile electronic Transactions forum (MeT) and the Intel mobile data initiative – next generation.

Further information regarding Blueice Research is available at: http://blueiceresearch.com or info@blueiceresearch.com

Securing Mobile Devices – Enabling Commerce

Why Mobile Devices?

Mobile devices are ideally suited to online commerce due to the fact that they are personal and have the ability to be connected to the network regardless of time or location. The ability of service providers and corporations to make information and corporate assets available to their customers and users at all times is compelling. It is the combination of these facts that also make them ideal for the storage of user digital credentials.

Mobile Device Security Needs

Due to their high availability and small size nature, mobile devices are more prone to being lost or stolen. This places a strong requirement on the protection of sensitive information stored in the device.

The security client, the Multipass, protects this sensitive information with strong encryption ensuring that only an authorised user can access the protected data.

Advanced Security Functionality

The Multipass security solution from Blueice Research presents an easily deployable cross-platform solution that allows users to strongly identify themselves, using their mobile devices, when accessing corporate information or on-line services from a mobile device or a traditional PC.

This ensures that applications that were previously only made available to the PC platform, due to a lack of security functionality on mobile platforms, can now be made available on such platforms without requiring a security compromise.

mCommerce Enablement

Thus, the Multipass is the mCommerce enabler application ensuring that on-line transactions, both from mobile devices and traditional PCs, are carried out using security solutions which provide ease of mind for both service providers and customers.

VBIC1.13

Blueice Research AB, Drottninggatan 71A , SE-11136 Stockholm, Sweden Telephone +46 8 545 51 880
Fax +46 8 545 51 881 E-mail: info@blueiceresearch.com Internet http://blueiceresearch.com/

Summary of functionality:

- Device encryption – the secure storage of private information
- Authentication – proof of user identity when using device
- One-time-password generation – compatible with existing infrastructure
- Digital signatures and receipts
- Service provider branding
- Multiple service and platform support
- Multiple browser support

Information Protection on the Mobile Device

The Multipass provides encryption functionality allowing for sensitive data to be encrypted using strong symmetric encryption on the mobile device. This is an elegant way to protect personal information and digital credentials. It ensures that if the device is lost or stolen, the infsormation contained within the Multipass will remain confidential.

User Authentication on the mobile Internet

When used in an on-line mode, for accessing corporate information or on-line services, the Multipass makes the crypto functionality available to the most commonly used browsers on the different devices via their plugin mechanisms. This means that the digital credentials within the Multipass can be used for user authentication.

One-Time-Password (OTP) Generation

The Multipass provides an OTP functionality. The generation of a one-time-password allows the user of the device to perform a stronger authentication than a mere static password can provide. The Multipass uses a challenge response mechanism in order to ensure the strong authentication. This functionality also ensures that, if there is an OTP system in place, the Multipass can support this system and provide and upgrade path to more advanced PKI systems.

Digital Signatures and Receipts

Users can digitally sign transactions on the Internet and also receive, verify and view digitally signed receipts.

Service Provider Branding

When accessing an online service, the user is presented with an interface personalised with the look and feel of the service being accessed. This ensures the preservation of online service branding and increases user confidence in the transactional situation.

Multiple Service Support

The Multipass can be used for accessing several different on-line services allowing users to use different digital credentials for the different systems.

Multiple Platform Support

The Blueice Research product is available on a variety of mobile platforms as well as on traditional PC platforms. This means that whatever platform the user is using, it will be possible to use the security functionality of the Multipass. It also allows service providers (merchants) and corporations to offer secure services on several different platforms.

Multiple Browser Support

The Multipass supports the most commonly used web browsers on the different supported platforms.

Free Multipass download from
http://blueiceresearch.com/multipass

Hardware and software support

Supported Client Platforms

- Palm OS 3.5 and higher
- PocketPC (Windows CE 3.0)*
- EPOC 32 R5 and higher*
- Windows NT 4.0, Windows 2000, Windows 95/98
- Linux*

* Release date to be announced

Supported Web Browsers

- Internet Explorer 4.0 and higher
- Netscape Navigator 4.0 and higher
- AvantGo 3.3 and higher

Standards compliancy

The Multipass conforms to the following cryptographic standards:

X.509v3	Certificate format
ANSI X9.57	DSA Signatures
RSA and DSA	Asymmetric encryption
MD5 and SHA1	Hash algorithms
Triple DES	Symmetric encryption
PKCS#1	RSA Encryption
PKCS#7	For signatures
PKCS#10	Certificate request
PKCS#11	Crypto token interface
PKCS#12	Token importation and exportation

Blueice Research AB, Drottninggatan 71A , SE-11136 Stockholm, Sweden Telephone +46 8 545 51 880
Fax +46 8 545 51 881 E-mail: info@blueiceresearch.com Internet http://blueiceresearch.com/