The Omlis Solution

Secure and highly efficient mobile transaction security

Introducing Omlis

Proven solutions, delivering unbreakable mobile transaction security.

Unlike all other commercially available encryption technologies, Omlis is designed specifically for the demands and dynamics of the mobile payments world.

Omlis brings to market a proven, highly powerful, differentiated and most effective solution to all mobile commerce security. Providing a completely secure, end-to-end, uncompromised, device-upward based encryption with 100% fault-tolerant tracking of all payments in real-time for full transaction accountability.

The Omlis architecture is extremely interoperable, enables rapid deployment and supports a massively scalable mobile payments network. Omlis transforms a network to offer instantly secure transactions and a greatly enhanced customer experience, providing absolute protection that's fraud-free and removing the need for additional peripherals; adding significantly more efficient throughput, resilience, and utilization of current infrastructure.

There are a number of compelling benefits that accelerate the adoption and growth of mobile payment services:

- Secure unbreakable encryption and a true one time key system
- Enhanced compliance for regulated markets, aiding rapid service deployment
- Interoperable between online and mobile environments in-line with market convergence
- Supports 3G, 4G mobiles and smart phone devices, as well as 2G due to small data packets size and reduced bandwidth demands
- Compatible with all existing security technologies
- Rapidly adoptable by legacy systems and invested networks across diverse markets and geographies
- Supports all transaction scenarios from EPOS, to mobile banking and merchant payments
- Using novel and proven dynamic authentication methods to ensure user identification cannot be faked, thus providing the utmost guarantee that the user is who they say they are
- Removing the single point of attack and empowering the mobile device to encrypt the data, spreading the risk profile throughout the mobile network

Market FAQs

What Is Omlis Addressing?

Omlis addresses all the major issues that impact on today's mobile payments market, most importantly the massive cost of fraud, which impacts everybody: institutions, businesses and individuals.

Why Should I Listen?

We have brought together a very reputable team with in-depth expertise in the mobile payments sector. We have developed a completely unique, patented and unbreakable encryption that resolves a host of major issues in an exciting market that is expected to grow from $235billion to $721billion in five years (Gartner).

Why Is Omlis Relevant?

Current encryption technologies are vulnerable to a growing range of specialized attacks. In 2014 estimated global cyber crime amounted to $575billion according to a report from McAfee and Intel.

What Does Omlis Solve?

We see our payment technology as a true enabler, offering rapid implementation of secure payment networks in both mature and emerging markets where there is a need for fresh thinking and a smarter approach to safe, secure and convenient mobile payments.

Not only does Omlis solve this problem, but due to its very nature it enables a far simpler and more elegant user experience. Our solution also dramatically reduces service delivery costs, unlocking potential profits.

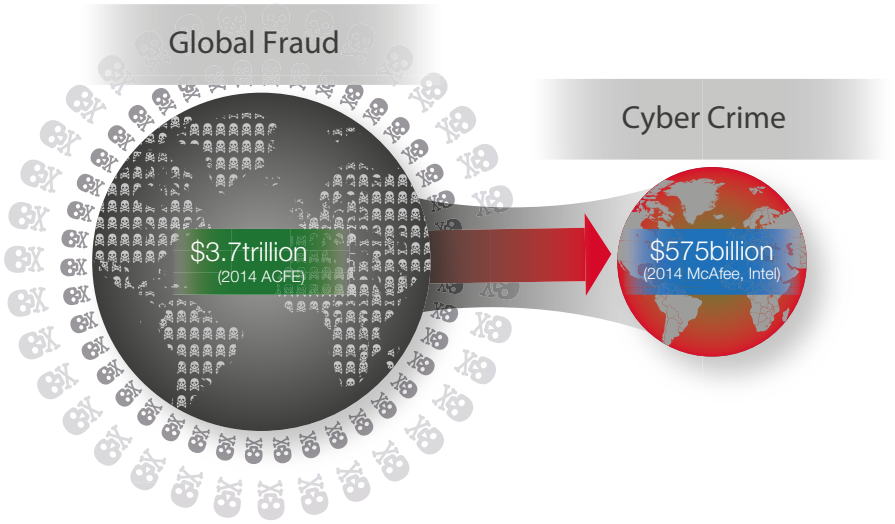
The Problem with Mobile Payments

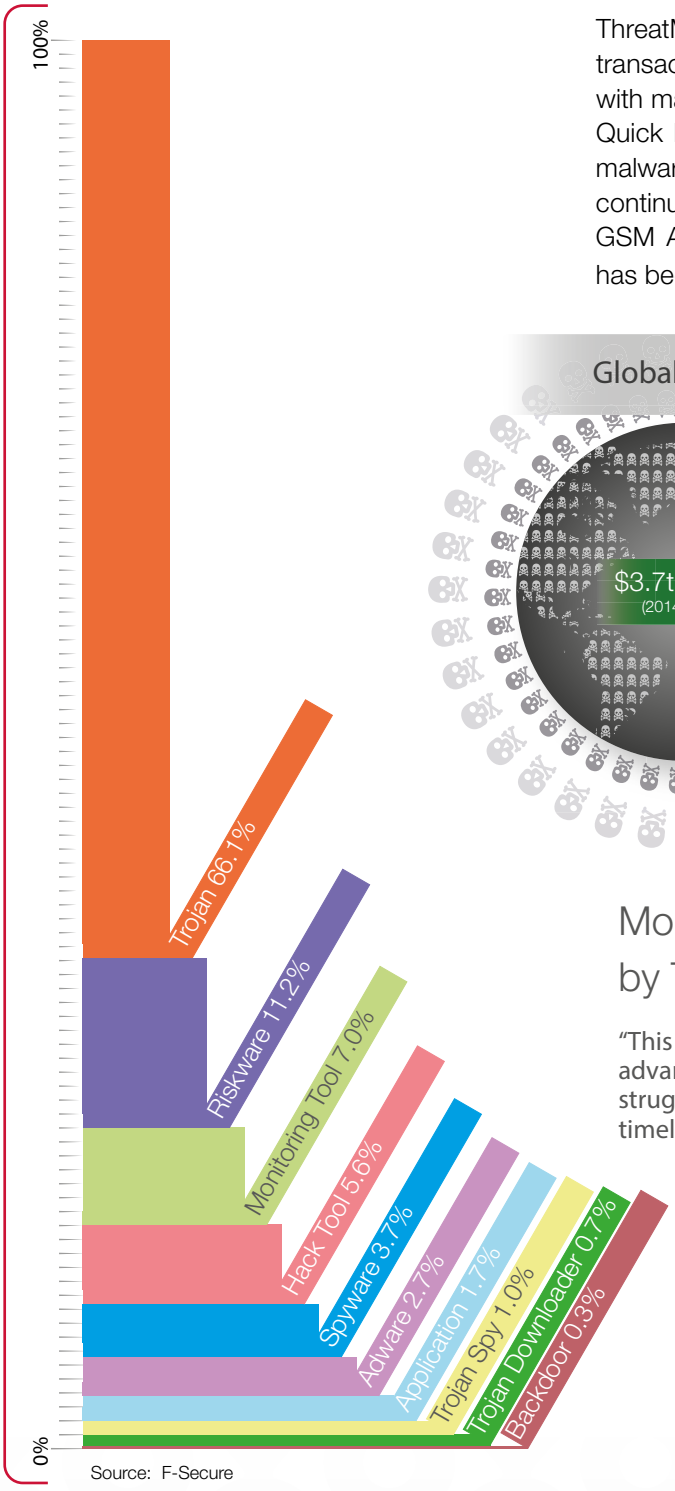
Fraud

Mobile payment solutions have enjoyed significant growth but fraud and, more specifically, trust remains a major constraint to realizing their full market potential. A global report published by Kount in 2014 states that an average of 32% of acquiring banks, card associations, card issuers, merchants and merchant service providers believe that the biggest barrier to mobile payment adoption are concerns about security.

The ACFE (Association of Certified Fraud Examiners) estimated in its 2014 Report to the Nations on Occupational Fraud and Abuse that nearly $3.7 trillion is lost to fraud worldwide – around 5% of 2013's gross world product of $70.8trillion.

ThreatMetrix highlights on average 5.85% of their transactions currently derive from compromised devices with many attacks now originating from mobile devices. Quick Heal data reports an increase of 30% in mobile malware attacks in 2012 alone. As mobile connections continue to grow - by 7.6% per year, according to the GSM Association - the need for more robust security has become critically important.





Source: F-Secure

Mobile Threats by Type (2012)

"This year, cybercriminals have become so advanced that security professionals are struggling to detect many of their attacks in a timely manner." (ThreatMetrix)

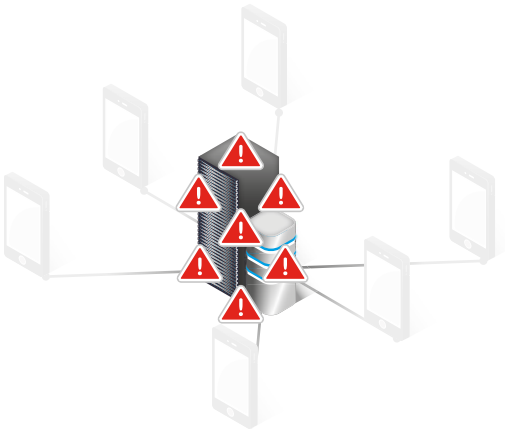
Consumer trust in mobile payments is significantly hampered by the impact and fear of fraud. By removing these concerns, consumer trust is gained and businesses can reap the benefits of enabling mobile payments.

Omlis Risk Profile vs Traditional Risk Profile

The Omlis solution, unlike other technologies, does not have a single point of failure. Traditional systems generally have a single point of failure where sensitive information is held - the hosted services that malicious parties can easily target. Omlis distributes the risk profile by displacing risk to the mobile device. The more devices that join a service, the smaller the risk profile without any compromise on the strength of the Omlis encryption system on the mobile device.

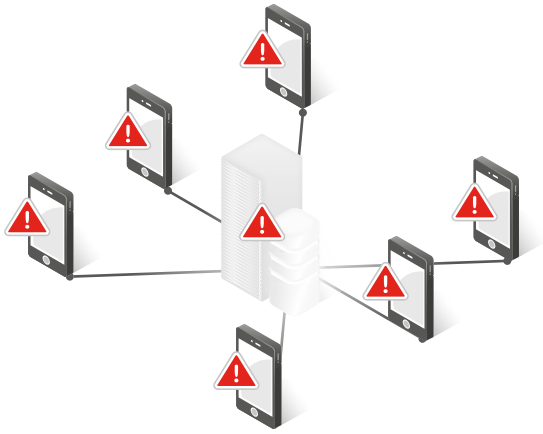
Normal Risk Profile

Single Point of Security Compr omise



Omlis Risk Profile

Spr ead Risk of Security Compr omise



Current Encryption

Section Summary:

- Fraud is dramatically increasing as mobile and internet centric payments increase
- Modern encryption systems are largely dependent on the protection of a single key
- Existing encryption solutions place a significant burden on servers and infrastructure

The transfer of sensitive information from one place to another is subject to increasingly costly criminal attack and incidents of committed fraud. This is a particular problem for payment systems using mobile devices which cannot be kept behind firewalls and for any kind of communication that must pass through an insecure network (such as the internet or mobile telephony infrastructure).

Modern encryption system methods that are currently employed to protect sensitive payments (such as Triple-DES and AES) are entirely dependent on the security of the keys that are used. These methods employ the same keys repeatedly giving criminals a significant opportunity to obtain a key by using cryptographic analysis of data. Keys can also be obtained by breaching security (through bribery, extortion, theft, etc.).

Modern encryption systems require additional protocols to facilitate the exchange of keys, representing further opportunity for compromise, while the multitude of keys required for large number of clients can also be problematic.

Existing encryption methods require significant processing power to decrypt data. This requires powerful and costly central server infrastructure to handle encrypted communications from a large number of devices. Additional servers may also be required to handle key exchange protocols, adding further to costs.

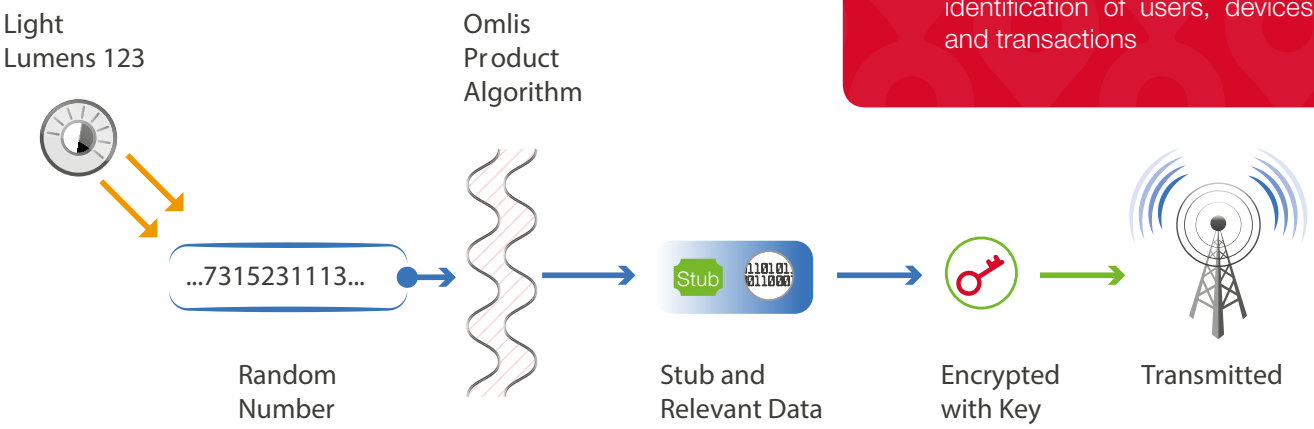
The failure and limitation of existing encryption technology processes questions the traditional ‘bigger is better’ encryption philosophy. Omlis understands the limitations of current encryption methodologies and offers an innovative solution that delivers a new encryption protocol offering unrivaled benefits.

Omlis Encryption Technology Outline

The Omlis encryption technology uses “one time key” encryption. This is used to encrypt small packets of data using unpredictable keys, which are generated by the mobile device.

Section Summary:

- Inherently secure encryption via “one time key”
- Truly random key generation using one-way transformations on environmental variables
- A key exchange is used for identification of users, devices and transactions



Each key is unique to a specific user, device and transaction. It is created, used and destroyed within a short time frame. This approach ensures minimal opportunity for data harvesting (to obtain keys) or for security to be breached. Secure, authenticated exchange of keys is an integral part of the Omlis communication protocol and thus no additional key-exchange infrastructure is required. A system of authentication keys, tickets and stubs is used to provide secure identification of the device from which communication originates.

The Omlis key generation method standardizes the use of random environmental variables across any mobile device regardless of make and model. Some variables are derived from user input, others will be variables associated with environmental conditions of the device.

Through the use of competition-winning cryptographic algorithms, proven within the industry, and a novel and efficient security architecture, Omlis keys and authentication ticketing cannot be predicted at all. The fact there is no master key eliminates the one possible attack against “one time key” encryption.

Security Strength

Section Summary:

- As computing power increases and cybersecurity criminal cartels become more organized, current encryption techniques become more vulnerable and easier to break
- The Omlis “one-time key” cannot be broken
- Omlis key generation occurs within the mobile device reducing the risk of attack on servers

The Omlis solution generates different encryption keys and authentication tokens for every transaction. Unlike other solutions on the market, these tokens and keys are not derived from a master-key. What this means is that malicious agents have no ability to execute identification theft and there is no possible route for them to steal payment detail in transit from the mobile device. It ensures unprecedented levels of security and traceability. The Omlis solution can guarantee that every transaction can be identified by the key and token pair.

Conventional encryption systems continue to support a model where the server remains a single-point-of-attack for malicious agents and criminal fraternities. The Omlis solution moves the focus of the end-to-end encryption of payment data from the server to the mobile device. This means the risk of server-side data breach is extremely small since keys and tokens are constantly being updated, there is no single attack-vector that can cause a mass breach.

The Omlis encryption technology offers security by utilizing a “one time key” for encryption. This encryption method will never become obsolete provided that the key generation for the “one time key” is seeded via truly random inputs, as is the case with Omlis.

Implementation

The Omlis encryption technology comprises of two main software elements. A client component is installed on the sending device; this generates keys and handles the communication protocol. This is termed the “Black Box” as it is protected from access by security measures. The “Black Box” communicates with the Omlis Managed Services installed on a server, which in turn manages keys and transaction tokens for all Omlis-enabled devices in a network.

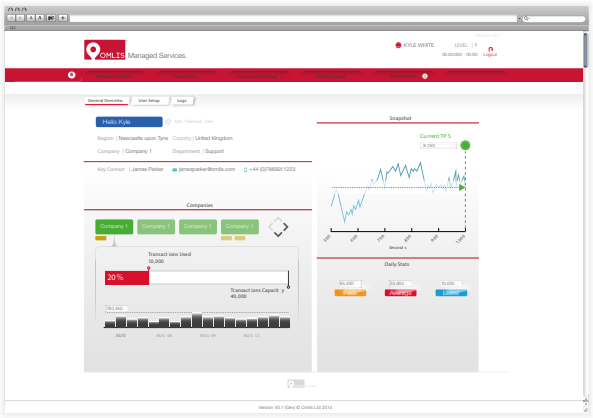
Software in the Omlis implementation has been developed using high-integrity software tools (SPARK Ada). These tools are typically used to develop safety-critical software used in aircraft, nuclear power stations and financial infrastructure. This approach ensures the Omlis software is not vulnerable to attacks, such as buffer-overflow that are used to breach the security of software developed using low-integrity tools.

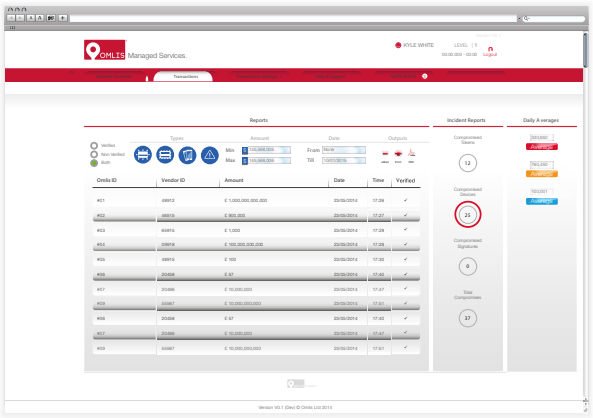
The Omlis Admin Portal

As an end-to-end mobile payment encryption solution, Omlis has developed an admin portal as a powerful tool that allows for the monitoring and management of Omlis encrypted payments. It is directly linked to the Omlis security protocol so that if any discrepancies or signs of attempted attack have taken place, the payment will be stopped and the user will be alerted of the fraudulent activity via the admin portal. These conditions are controlled by protocols that are controlled in the administration part of the Omlis managed services.

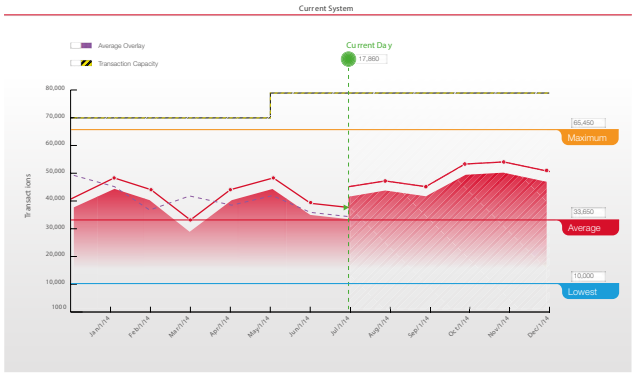
Feature Highlights

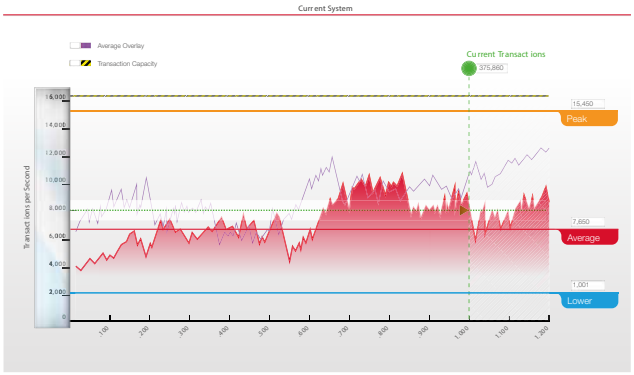
- Allows for the management and real time monitoring of Omlis encrypted transactions
- Allows the export of data to support big data analytics

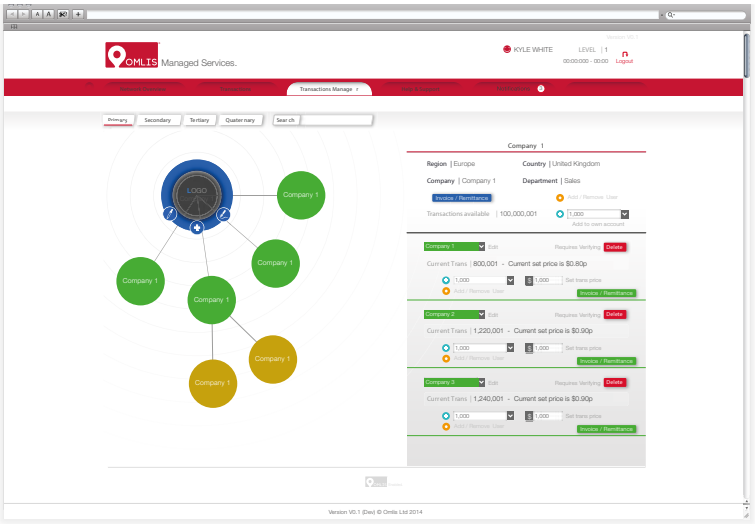




- Instant visibility on transaction values
- Trend analysis with predictive capability







- Monitoring of the performance of reseller implementations
- Access control provision, supporting data restrictions to different management levels

Conclusion

Omlis protocols represent a paradigm shift in mobile payment security offering a multitude of unrivaled benefits over existing encryption solutions. Omlis is feature rich whilst being extremely user and business friendly. The Omlis approach brings massive ROI compared with existing solutions and has been designed to protect all stakeholders in the payments ecosystem now and in the future.

V1.5 - 01.2015

Abbrevia Head Office, Dubai
+971 4 365 4777

Abbrevia Moscow, Russia
+7 495 995 0939

Abbrevia Saudi Arabia, Riyadh
+966 11 406 6927

For more information please visit our website
www.abbrevia.com

or email us at
info@abbrevia.com