PRIVATE POST
signed sealed delivered

White Paper

SK-KEM: Sakai Kasahara Key Exchange Mechanism

This paper examines the differences between the four generations of cryptography and explains why only fourth generation solutions are equipped for a sustainable role in modern communication.

ENCRYPTION – NOT THE REAL CHALLENGE

Around the world companies are competing to develop ever stronger encryption systems. They are missing the point. Already we have the Advanced Encryption Standard (AES) which is widely acknowledged as having no known weaknesses. With AES-256 there are 2^{256} possible keys. That equates to 77 zeros, so the number of different keys a potential cracker would have to try is more than 100,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000,000.

The odds are heavily stacked against anyone breaking AES - even with the fastest computers available today it would take billions of years to try all the possibilities.

As computers get faster, using a longer AES key evens the balance. Since data can be encrypted so securely with AES, the only question that remains is how two people exchange keys safely without the risk of eavesdropping.

ASYMMETRIC KEYS

First generation crypto systems use the same key to both encrypt and decrypt the message. Julius Caesar created the first known symmetric cipher system which rotated letters in the alphabet and had only 26 possible combinations. The AES system described above is its modern equivalent.

The second generation of crypto systems were devised to try to offer a solution to the key exchange challenge. They are known as asymmetric systems because different keys are used for encrypting and decrypting data. Probably the best known system for asymmetric encryption is PGP (Pretty Good Privacy). Such asymmetric systems are also often referred to as PKI (Public Key Infrastructure), which describes the systems infrastructure that is required to support them, rather than the cryptography itself. In an asymmetric system keys are generated in pairs – a non-secret public key is used to encrypt data which can only be decrypted using the corresponding secret private key. Where these systems break down is that they require pre-enrolment, so everyone to whom you want to send a message must be set up on the same system as you before you send the message.

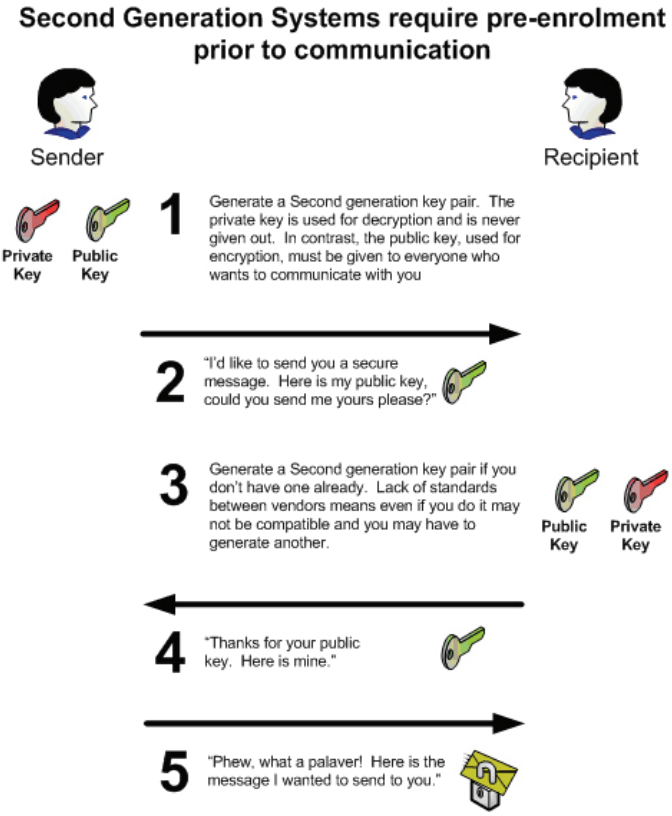
To use a second generation system you need to get an independent public key for every person in your address book. That's complicated enough but then consider what happens if someone loses a key. In a perfect world all your contacts would have their keys backed up but in reality many of them won't. This means that every time you send a message you need to check that the public key you have really is the most recent one.

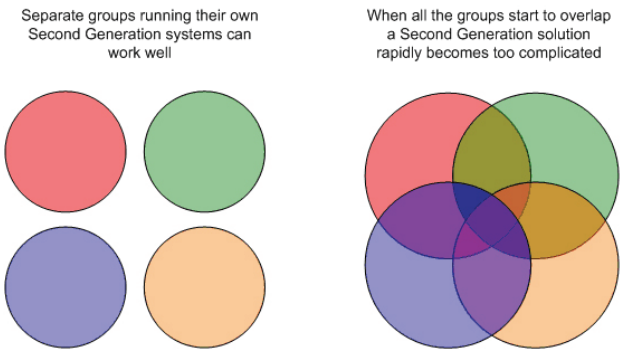
PRIVATE POST PROTECTED

Identum™
Protecting Privacy

The solution from the computer industry has been to add infrastructure. Many different vendors have supplied boxes to manage keys, each aiming to automate the process of checking that they always have the latest keys for everyone in their organisation. However, despite systems being commercially available from major vendors for several years, only a fraction of email traffic is currently encrypted. This is because people are not used to operating in isolated groups. Each one of us exists within lots of different groups that criss-cross and overlap with others. In 1929, in a short story called "Chains", the Hungarian writer Frigyes Karinthy proposed the theory of six degrees of separation. He suggested that any two people are connected by a chain of, at most, five intermediate acquaintances. His theory has since been tested and found to be accurate.

The new infrastructure has done nothing more than add complexity. Key management boxes only help when you want to talk to someone who happens to be sharing the same infrastructure as you, and you are online connected to that infrastructure.





BACK TO THE DRAWING BOARD...

What is needed is a system that allows you to securely encrypt data to an email user based on a public key that is already public knowledge. What could be more obvious than the user's email address? Ideally you should be able to encrypt to several email users at once without multiplying out the size of the email, and each of them should be able to reply to all or any in the normal way.

THIRD GENERATION SYSTEMS – NOT QUITE THERE

In 1984 Adi Shamir (perhaps best known as the S from RSA) proposed a system called identity based encryption (IBE). Unfortunately, he couldn't solve the mathematics to make it happen. IBE uses a well known public identity to seed an encryption algorithm. It took until the turn of the century for two Japanese mathematicians, Ryuichi Sakai and Masao Kasahara, to make a breakthrough. This allowed cryptographers in England and the USA to design the first commercial implementations of identity based encryption which has become known as third generation cryptography.

Unfortunately, in the rush to market IBE several key areas were skipped. It was forgotten that the real problem is not encryption but key exchange. Third generation systems deliver security and improve key exchange, but they do so at the expense of performance.

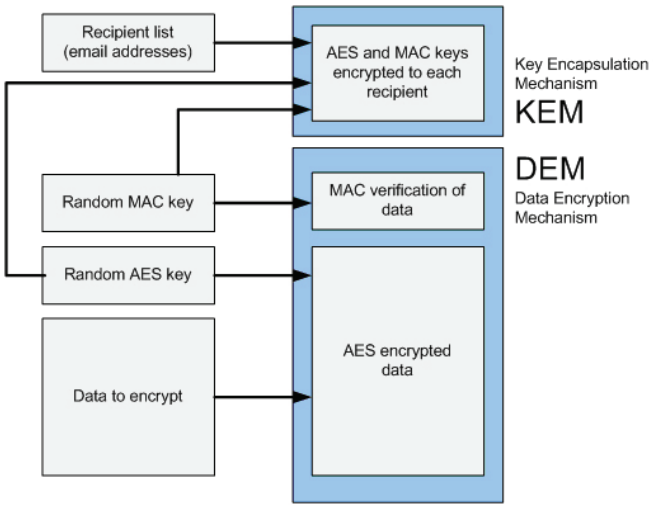
In essence the only improvement between second and third generation was removing the need for pre-enrolment. The third generation was modelled on the second generation and duplicated the flaw of creating islands of cryptography that allow users to enrol after receiving a message but then requires them to enrol with each of the closed groups they want to participate in.

KEM & DEM

Let's go back to AES. While it is the world's leading encryption system it is not the best solution for key exchange. A next generation solution is to couple AES as the data encryption mechanism (DEM) with a sophisticated key encapsulation mechanism (KEM) to provide an AES key exchange system.

AES is particularly quick at encrypting and decrypting so it can deal with large files without slowing down the user. Its high level security is enhanced when a different AES key is used for every message. The same AES key can be used for each recipient of a message which means one (encrypted) copy of the message body and any attachments, irrespective of how many recipients the email is sent to.

In context of typical email messages, even a key with 2^{256} possible permutations is relatively short, so encrypting that key to each recipient adds very little data overhead to the email.



FOURTH GENERATION CRYPTOGRAPHY – A SOLUTION FOR THE REAL WORLD

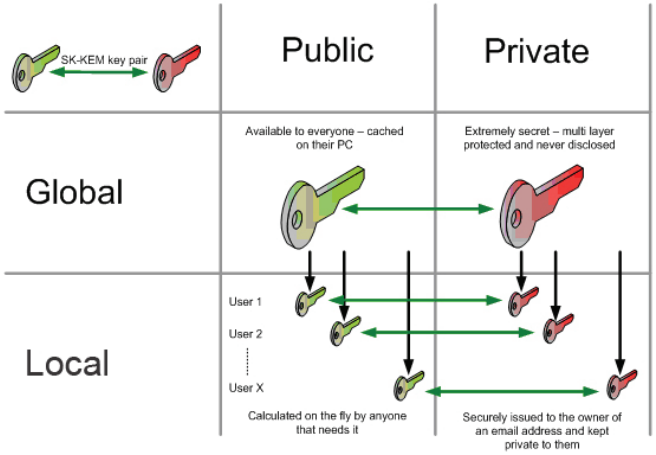
A fourth generation system combines the strengths of each of the three previous generations. It requires no pre-enrolment and the minimum of key handling. It uses multiple key pairs in just the same way as a second generation system with one vital difference: in a fourth generation system the key pairs are all securely related. Anyone with an email address can encrypt a message to anyone else, or to groups of people, knowing only the email address of the recipient(s) and a single global master public key. They can be offline and still encrypt their message, ready to be sent when they next connect to their mail server. The recipient does not need to pre-enrol before receiving fourth generation encrypted messages. This is the ideal encryption system. It is highly secure with minimal key handling and virtually no data overhead, even on large messages sent to many recipients. Implementation of SK-KEM enables users to add encryption to their email with a single click, or even set an option in their email program to encrypt every message in the background.

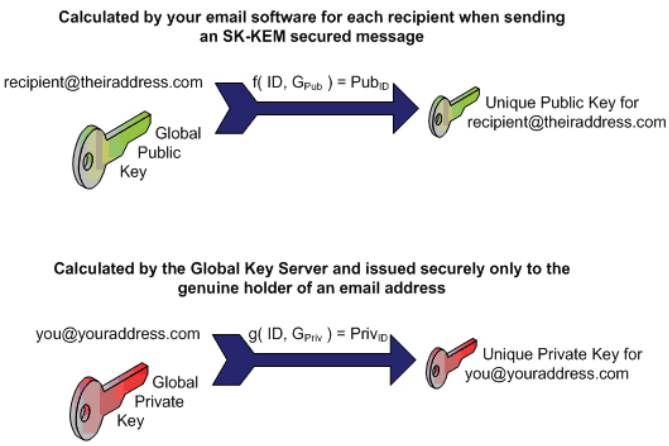
THE SAKAI KASAHARA KEY ENCAPSULATION MECHANISM (SK-KEM)

Fortunately Sakai and Kasahara didn't rest on their laurels when they solved the mathematics that gave rise to the third generation of cryptography. They carried on enhancing the maths to make it more elegant and simpler to calculate. SK-KEM has grown out of that work and is the ideal solution to the key exchange challenge. It provides a way to calculate a unique public key for any email user based on their email address and a single global public key. This key can be calculated by any sender at any time without the recipient having to be involved.

In effect, with the SK-KEM system every past, present and future email user on the planet already has a unique public key even if they don't yet realise it. Each of these public keys has a corresponding private key which can be issued to the owner of an email address before or after they receive their first encrypted message.

The diagram on below illustrates the process of calculating an SK-KEM public and private key pair. For more details on the mathematics involved we recommend viewing the white paper entitled An Efficient ID-KEM Based on the SK Key Construction, co-authored by Prof Nigel Smart, one of the members of our Advisory Board, which can be found at www.privatepost.com/ourtechnology/ID-KEMwhitepaper.pdf.





PRIVATE POST™
signed sealed delivered

White Paper

The power of the maths developed by Sakai and Kasahara is in making sure that near perfect knowledge is not enough. You might know all of the public information and all of the formulae for how SK-KEM works. You might even register many email addresses and be issued with many private keys. However, without the global private key you cannot calculate someone else's private key, and without that you can't read their email.

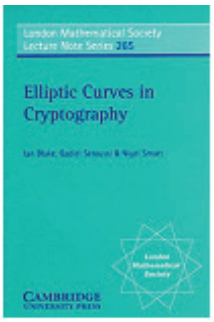
This is possible because the system is built on top of elliptic curve cryptography (ECC). Widely acknowledged as the best cryptographic backbone system available, the US National Security Agency says, "The United States, the UK, Canada and certain other NATO nations have all adopted some form of elliptic curve cryptography for future systems… Elliptic curve cryptography provides greater security and more efficient performance".

ELLIPTIC CURVES

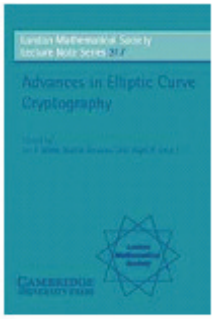
An elliptic curve is a precisely defined mathematical shape.

Carefully chosen elliptic curves have special properties that can be used to produce the one way formulae that are essential to modern cryptography. A one way formula allows for the result to be calculated precisely in one direction only. In the opposite direction the result cannot be calculated but must be guessed at by a process of trial and error in an effort to stumble across the correct answer. By making the number of possible answers so vast it would take trillions of years to test them all, a formula is created that is effectively irreversible.

There are many comprehensive references available on elliptic curve cryptography, two of which were co-authored by Professor Nigel Smart of Bristol University, one of the creators of SK-KEM and a member of the Identum advisory board.



ISBN: 0521653746



ISBN: 052160415X

CONCLUSION

SK-KEM is more than a fourth generation crypto system that solves key exchange problems without adding complexity to the user. When the internet was originally assembled 30 years ago, the people involved knew that data must be encrypted and authenticated but they didn't know how to do it, nor could they foresee that the world would come to rely on electronic communication.

Today Identum is retro-fitting the vital security that is missing from the internet's infrastructure, pioneering secure internet communication for the 21st Century without which no business will survive. This is the only sustainable way forward. There is no going back.

HQ/Europe
Identum
The Quad
Stubbings Estate
Henley Road
Maidenhead
Berkshire
SL6 6QL
United Kingdom
+44 (0)1628 82 82 80
euinfo@identum.com

North America
Identum
13800 Coppermine Road
3rd Floor
Herndon
Virginia 20171
United States
+1 703 234 7916
usinfo@identum.com

Asia Pacific
Identum
17/F The Kwangtung
Provincial Bank Building
409 Hennessy Road
Wanchai
Hong Kong
+852 2591 1801
apinfo@identum.com

Australasia
Identum
PO Box 5066
West Chatswood
Sydney
New South Wales
1515
Australia
+61 (2) 9410 9965
ausinfo@identum.com

www.privatepost.com
www.identum.com

Identum™
Protecting Privacy