

User-Friendly Digital Signatures

Jon Matonis, CEO, Hush Communications

Digital Identity Forum

October 17 & 18th 2000

Marlborough Hotel

London, UK

October 23, 00

Copyright 2000 Hush Communications

Overview

- Digital Signatures & the Market
- What are Digital Signatures ?
- Signatures v. Certificates
- Complex PKI Deployments
- The Hush Communications Solution: Technology
- The Hush Communications Solution: Trust
- Contact Hush

October 23, 00

Copyright 2000 Hush Communications

Digital Signatures & the Market

- Until recently, digital signatures were not considered legally binding within the United States;
- Europe has been quicker to adopt digital signatures as a replacement for the traditional written signature;
- Touted as the link between consumers and e-commerce, digital signatures are an emerging technology poised to generate significantly larger transaction sizes.

October 23, 00

Copyright 2000 Hush Communications

What are Digital Signatures ?

- Digital signatures verify with mathematical certainty that the message, document, or other media received originated from the anticipated sender (authentication);
- Digital signatures ensure that what you send over the Internet is exactly what is received at the other end (integrity);

October 23, 00

Copyright 2000 Hush Communications

What are Digital Signatures ?

- Digital signatures ensure that someone cannot deny that they authorized a particular transaction (non-repudiation);
- There are multiple ways to create digital signatures, including biometrics, like face printing and retina scans, but the most common methods involve cryptographic algorithms and protocols.

October 23, 00

Copyright 2000 Hush Communications

Signatures v. Certificates

- A digital signature is created by encrypting data with a private key.
- A digital certificate is a public key that is digitally signed by a Certificate Authority (CA).

October 23, 00

Copyright 2000 Hush Communications

Complex PKI Deployments

- Issuing a digital certificate can cost anywhere from \$5 to \$10 per customer.
- The enterprise software needed to manage the key, which decrypts and encrypts a message, can cost as much as \$10 to \$100 a person.
- Consumers must pay a periodic fee for the use of a digital certificate.
- Most signing devices are linked to a particular PC or network.

October 23, 00

Copyright 2000 Hush Communications

Complex PKI Deployments

- The private portion of the digital identity must be accessible exclusively to the owner and must be used to decrypt and sign data.
- Most PKI solutions require that the user possess their private key, which is inherently unsafe and reliant upon properly configured hardware.

October 23, 00

Copyright 2000 Hush Communications

Complex PKI Deployments

- PKI-based digital certificates are inefficient and cumbersome where a certificate is required to authenticate an individual user.
- Traditional PKI doesn't have roaming capability.

The Hush Communications Solution

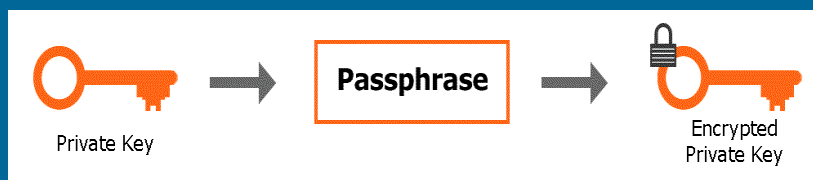
The Hush Encryption Engine™ allows end-users to store their private key on a Hush server. The user doesn't have to carry a private key, smart card, or store the key on a hard drive. However, even though Hush manages the private key, it is always encrypted and is inaccessible to anyone at Hush or elsewhere.

The Hush Communications Solution

- The Hush Encryption Engine™ ensures that no one but you can access your private key.
- The Engine doesn't tie you to a single computer.
- The Engine is compatible with multiple online applications.
- The Engine works with the Java™ technology in most common Web browsers.

Hush Technology

- Hush users generate their private key on their own computer first, during signup of installation, and encrypt it with a passphrase.



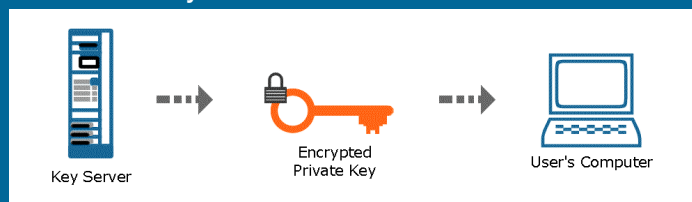
Hush Technology


- And then, upload the encrypted private key to one of the Hush servers.



Hush Technology

- After that, whenever a user starts a secure communications session, the private key automatically is retrieved from the server.




Hush 

Page 15


Hush Technology

- And finally, decrypted with the user's passphrase.



Encrypted Private Key → **Passphrase** → Private Key

October 23, 00
Copyright 2000 Hush Communications


Hush 

Page 16

IMPORTANT SECURITY NOTE

- When the private key resides on a Hush key server, it is encrypted with a passphrase. That passphrase NEVER leaves the user's computer. At no point is the private key or any private data accessible to anyone at Hush. Even if Hush were to be subpoenaed, we would not be able to learn or reveal your private key.

October 23, 00
Copyright 2000 Hush Communications


Hush 

Page 17

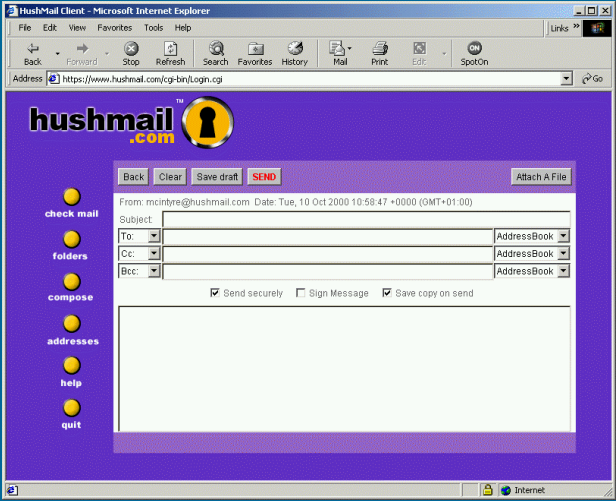
Hush Digital Signatures

- Hush offers its users the option to digitally sign their email and attachments.
- Hush's digital signature feature is a method for the individual user to authenticate their online identity.

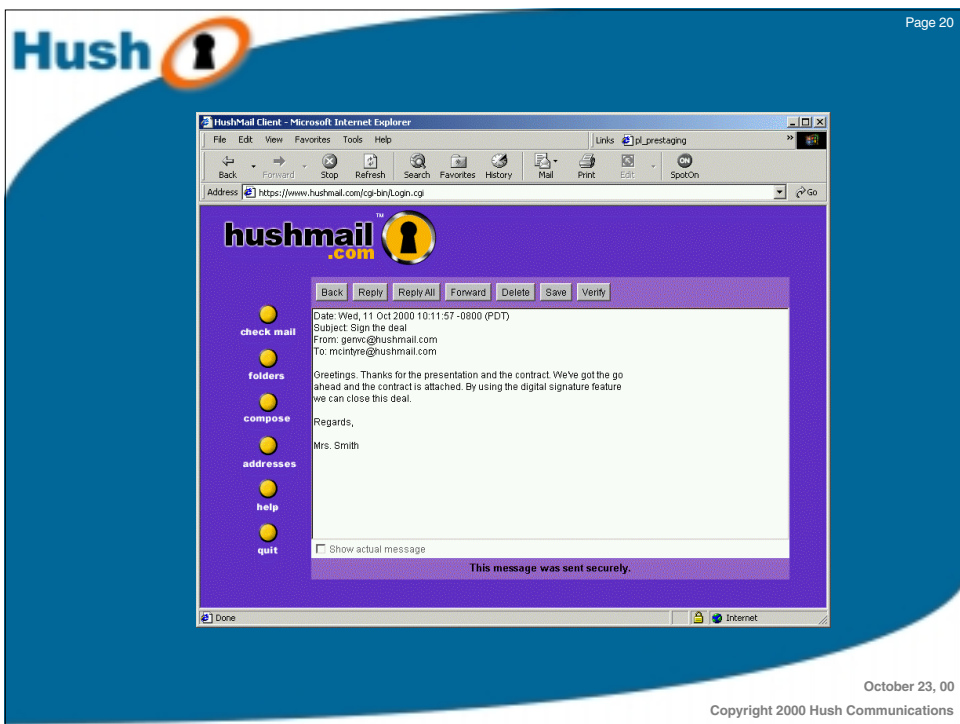
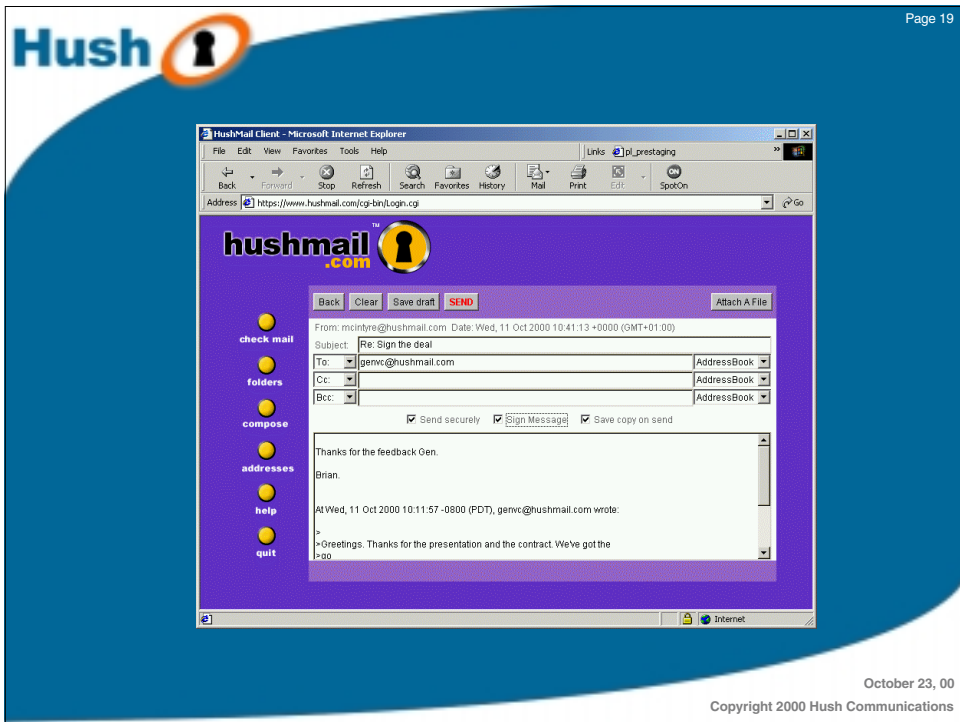
October 23, 00
Copyright 2000 Hush Communications

Hush 

Page 18

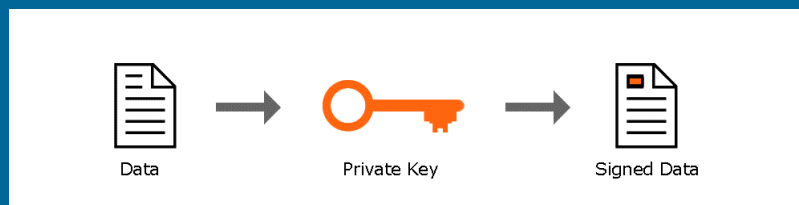


October 23, 00
Copyright 2000 Hush Communications



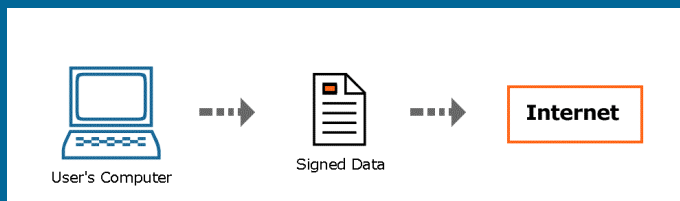
Sending a Digitally Signed Message

- First, the data is signed with the user's private key, which the user retrieved at the start of the session, when the user logs in with their passphrase.



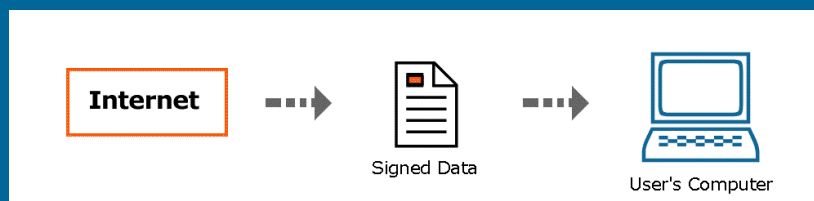
Signed Message is Transmitted

- Then, the signed data is sent on to its final destination.



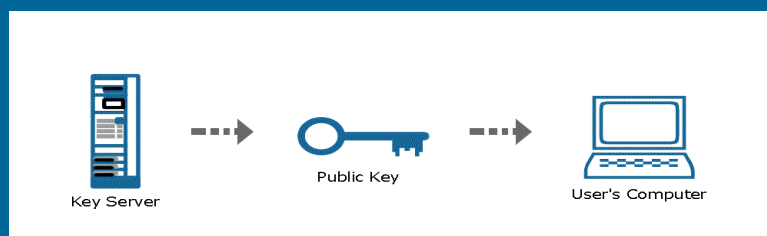
Verifying a Digitally Signed Message

- First, the signed data arrives at the recipient's computer.



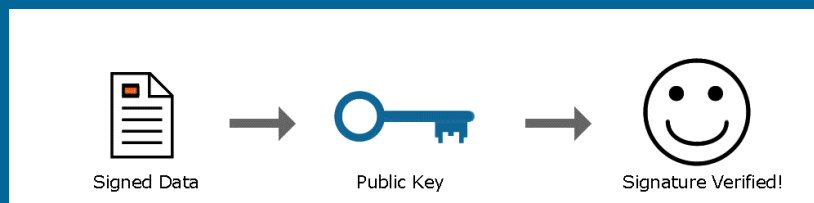
Verifying a Digitally Signed Message

- Then, the sender's public key is automatically retrieved from a Hush key server.



Verifying a Digitally Signed Message

- Finally, the public key is used to verify the authenticity and integrity of the data.



The Hush Communications Solution

- Hush offers Private Label services as a way for leading companies to brand their secure messaging.
- Trusted Private Label partners control the registration and revocation process.
- Digital signatures are enforced and backed up by the policies of the Private Label partner.



Contact Hush Communications

Worldwide

Headquarters

Hush Communications
22 Upper Pembroke St.
Dublin 2, Ireland
Phone +353-1-241-0303
Fax +353-1-241-0370
alliances@hushmail.com

Sales & Business

Development Office

Hush Communications
2825 E. Cottonwood
Parkway, Ste. 500
Salt Lake City, UT 84121
Phone +801-990-3490
Fax +801-990-3111
sales@hushmail.com